Université de Montréal

La surveillance de l'utilisation d'Internet au travail : guide des droits et obligations des employeurs

Par
Sophie Rompré

Faculté de droit

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de Maîtrise en droit
option droit des technologies de l'information (LL.M.)

Juin, 2009

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :

La surveillance de l'utilisation d'Internet au travail : guide des droits et obligations des employeurs

présenté par :
Sophie Rompré

a été évalué par un jury composé des personnes suivantes :

Renée-Claude Drouin
président-rapporteur

Pierre Trudel
directeur de recherche

Karim Benyekhlef
membre du jury

RÉSUMÉ

Tout employeur qui fournit l'accès Internet au sein de son entreprise a intérêt à surveiller l'usage qui en est fait par ses employés, que ce soit pour maximiser les avantages ou pour réduire les risques liés à l'utilisation d'Internet au travail. Tout employeur a d'ailleurs le droit d'exercer une telle surveillance, sous réserve toutefois des droits des personnes surveillées.

La mise en place d'une surveillance de l'utilisation d'Internet au travail peut porter atteinte à la vie privée des employés ou à leur droit à des conditions de travail justes et raisonnables, et peut également porter atteinte au droit à la vie privée des tiers indirectement visés par la surveillance. Dans ce contexte, afin de s'assurer que la surveillance est exercée dans les limites de ses droits, l'employeur doit franchir deux étapes de réflexion essentielles.

L'employeur doit en premier lieu déterminer le niveau d'expectative raisonnable de vie privée des personnes surveillées, lequel niveau s'apprécie à la lumière d'une série de facteurs. L'employeur doit par ailleurs respecter les critères de rationalité et de proportionnalité. Ces critères requièrent notamment que l'employeur identifie les motifs sous-jacents à la surveillance ainsi que la manière dont la surveillance sera exercée. Une fois ces deux étapes franchies, l'employeur sera en mesure d'identifier les obligations auxquelles il est soumis dans le cadre de la mise en place de la surveillance.

Mots clés : Surveillance au travail – Internet – Vie privée – Condition de travail – Rationalité – Proportionnalité – Renseignements personnels – Obligation d'information – Consentement – Politique.

ABSTRACT

All employers providing Internet access to their employees should implement Internet monitoring in the workplace, to increase the benefits and reduce the risks related to Internet use at work. Employers have the right to implement this kind of monitoring subject, however, to the rights of employees and third parties.

The implementation of Internet monitoring within the workplace can affect employees' privacy and the right to fair and reasonable conditions of employment, as well as the rights of third parties who may be indirectly subject to monitoring. In this context, the employer should go through two steps of reasoning.

The employer should first determine the level of reasonable expectation of privacy of all individuals monitored, which level is assessed in the light of numerous factors. The employer must also meet the criteria of rationality and proportionality. These criteria require that the employer identifies the reasons behind monitoring, and how monitoring will be exercised. After these two steps, the employer will be able to identify the obligations to which he is submitted through the implementation of Internet monitoring.

Key Words : Workplace monitoring – Internet – Privacy – Conditions of employment – Justification – Proportionality – Personal Information – Obligation to inform – Consent – Policy.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES SIGLES ET ABRÉVIATIONS

A.2d :	Atlantic Reporter 2nd Series
al.	alinéa(s)
ABQB :	Cour du Banc de la Reine de l'Alberta
A.F.C.C.A. :	United States Air Force Court of Criminal Appeals
A.G. N.U. :	Assemblée Générale des Nations Unies
A.J. :	Alberta Judgments
A.L.R. :	American Law Reports, 5th Series
Alta. L.R. :	Alberta Law Review
A.P.R. :	Atlantic Provinces Reports
A.R. :	Alberta Reports
art. :	Article(s)
B.C.C.A.A.A. :	British Columbia Collective Agreement Arbitration Award
B.C.J. :	British Columbia Judgments
B.C.W.L.D. :	British Columbia Weekly Law Digest
B.E. :	Banque Express
B.L.R. :	Business Law Reports
Bull. civ. :	Bulletin des arrêts des chambres civiles de la Cour de cassation
C.A. :	Cour d'appel ou Recueil de la Cour d'appel
C.A.A.F. :	Court of Appeals for the Armed Forces (USA)
C.A.I. :	Commission d'accès à l'information
Can. Arb. Bd. :	Canadian Arbitration Board
CarswellNS	Banque de données de WestlaweCarwell (Nova Scotia)
CarswellAlta	Banque de données de WestlaweCarwell (Alberta)
C.c.Q. :	Code civil du Québec
C.Cr. :	Code Criminel
CF :	Cour fédérale
C.H.R.R. :	Canadian Human Rights Reporter
ch. Soc. :	Chambre sociale

Cir. :	Circuit
C.L.A.D. :	Canada Labour Arbitration Digest
Comp. La. L. & Pl'y J. :	Comparative Labor Law & Policy Journal
conf. par :	confirmé par
contra :	contrairement à
C.P.R. :	Canadian Patent Reporter
C.R.T. :	Commission des relations du travail
C.R.T.F.P. :	Commission des relations de travail dans la fonction publique
C.Q. :	Cour du Québec
C.S. :	Cour Supérieure
C.S. Can. :	Cour Suprême du Canada
C.S.I. :	Computer Security Institute
C.T. :	Jurisprudence en droit du travail. Décisions des commissaires du travail
D.E.A. :	Diplôme d'études approfondies
dir. :	Directeur de publication
D.L.R. :	Dominion Law Reports
D. Mass. :	District of Massachusetts
D.OR. :	District of Oregon
DORS :	Décrets, Ordonnances et Règlements Statutaires
Doc. Off. A.G. N.U. :	Document officiel de l'Assemblée générale des Nations Unies
D.T.E. :	Droit du travail Express
éd. :	édition
E.D. Penn.	Eastern District of Pennsylvania
Employee Rts. & Emp. Pol'y J. :	Employee Rights and Employer Policy Journal
et suiv.	et suivant(e)(s)
F.B.I. :	Federal Bureau of Investigation
F.3d :	Federal Reporter (3rd Series) (USA)
F. Supp. :	Federal Supplement (USA)
Harvard L.Rev. :	Harvard Law Review

inf. par :	infirmé par
infra :	Plus bas
J.E. :	Jurisprudence Express
JORF :	Journal officiel de la République française
L.A.C. :	Labour Arbitration Cases
L.C.	Lois du Canada (depuis 1987)
L.n.t. :	Loi sur les normes du travail
L.Q. :	Lois du Québec
L.p.r.p. :	Loi sur la protection des renseignements personnels
L.p.r.p.d.é.v	Loi sur la protection des renseignements personnels et les documents électroniques
L.R.Q. :	Lois refondues du Québec
L.R.C. :	Lois révisées du Canada (depuis 1985)
M.J. :	Military Justice Reporter
n° :	numéro
N.U. :	Nations Unies
NBQB :	Cour du Banc de la Reine du Nouveau-Brunswick
N.B.R. :	New Brunswick Reports
N.D. Ill. :	Northern District of Illinois
O.J. :	Ontario Judgments
Ont.	Ontario
O.R. :	Ontario Reports
p.	page
par. :	paragraphe
Pa. Super :	Pennsylvania Superior Court
P.U.L. :	Les Presses de l'Université Laval
QCCRT :	Commission des relations du travail du Québec
QCCA :	Cour d'appel du Québec
QCCQ :	Cour du Québec
QCCS :	Cour Supérieure du Québec
R.C.S. :	Recueil de la Cour Suprême
R.D. McGill :	Revue de droit de McGill

R. du. B. :	Revue du Barreau
Rés. A.G. :	Résolution de l'Assemblée générale
R.J.D.T. :	Recueil de jurisprudence en droit du travail
R.J.Q. :	Recueil de jurisprudence du Québec
R.P.C. :	Reports of Patent Cases (Australia)
R.R.A. :	Recueil en responsabilité et assurance
R.T.N.U. :	Recueil des Traités des Nations Unies
R.-U. :	Royaume-Uni
S.A.G. :	Sentences arbitrales, griefs
S.D. Ohio :	Southern District of Ohio
S.F.P.B.Q. :	Service de la formation permanente du Barreau du Québec
Soc. :	Cour de Cassation – Chambre sociale
Stan. Tech. L. Rev :	Stanford Technology Law Review
S.T.E. :	Série des Traités Européens
supra :	Plus haut
t. :	tome
T.A. :	Tribunal d'arbitrage
T.D.P.Q. :	Tribunal des droits de la personne du Québec
Trib. Gr. Inst. :	Tribunal de Grande Instance
U.R.L. :	Uniform Resource Locator
U.S. Dist. Ct. :	United States District Court
U. Toronto Fac. Law Rev. :	University of Toronto Faculty of Law Review
vol. :	volume
WL:	WestLaw
W.W.R. :	Western Weekly Reports

Remarque

L'emploi du mot « Code civil du Québec » réfère au *Code civil du Québec*, L.Q. 1991, c. 64, entré en vigueur le 1er janvier 1994 (C.c.Q.)

À la mémoire de ma mère.

REMERCIEMENTS

Je tiens tout d'abord à remercier Guillaume pour son support, mon père et ma sœur qui m'ont soutenu tout au long de ma maîtrise, Alex, Aleks, Marie-Ève, Karoline, Geneviève et Hélène pour leurs encouragements, ainsi que Sylvie, pour ses précieux commentaires et corrections. Aussi, je tiens à exprimer mes profonds remerciements à mon directeur de recherche, le professeur Pierre Trudel pour son aide précieuse, sa patience et ses encouragement, et surtout pour m'avoir permis de réaliser le présent mémoire. Finalement, je tiens à remercier ma mère qui m'a accompagné, encouragé et soutenu pour une bonne partie de la rédaction de ce mémoire, et qui a su me transmettre l'énergie nécessaire pour le compléter.

INTRODUCTION

> « [S]ouvent, la surveillance électronique est comme utiliser un canon pour tuer une mouche »[1]

L'employeur québécois qui décide de surveiller les activités Internet de ses employés au travail dispose actuellement de très peu de ressources juridiques lui indiquant clairement comment s'y prendre sans porter indûment atteinte aux droits des employés et quels sont ses droits et obligations à l'égard de ce type de surveillance.

Malgré le fait que les employeurs surveillent l'utilisation d'Internet de leurs employés depuis maintenant plus d'une dizaine d'années, la doctrine québécoise sur le sujet se limite, jusqu'à aujourd'hui, à énoncer les enjeux soulevés par la surveillance de l'utilisation d'Internet au travail, particulièrement au niveau de la vie privée des employés, sans toutefois fournir des balises claires quant à la façon d'atteindre un équilibre entre les différents intérêts en jeu.

Bien que les employeurs puissent retrouver, dans la doctrine, certaines recommandations générales quant aux mesures à prendre lors de la mise en place d'une surveillance de l'utilisation d'Internet, rien n'indique spécifiquement si ces recommandations constituent de réelles obligations et ce, en vertu de quelles sources juridiques, et si l'employeur peut être soustrait à ces obligations dans certaines situations.

Par ailleurs, les décisions québécoises sur le sujet se comptent sur les doigts de la main et ne permettent pas d'établir des principes généraux applicables dans toutes les circonstances. La jurisprudence québécoise actuelle ne fournit donc pas un meilleur

---

* Les références électroniques mentionnées ci-après sont à jour au 29 juin 2009.

1 COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La vie privée au travail à l'ère d'Internet*, discours de George Radwanski, Toronto, 4 octobre 2002, en ligne : http://www.privcom.gc.ca/speech/02_05_a_021004_2_f.asp.

éclairage aux employeurs quant à la façon de mettre en place une surveillance de l'utilisation d'Internet au travail.

Malgré tout, la surveillance de l'utilisation d'Internet en milieu de travail est devenue pratique courante au sein des entreprises et ce, depuis déjà plusieurs années. Dans ce contexte, et compte tenu du manque de ressources juridiques, il est légitime de croire que les employeurs n'ont eu d'autres choix que d'établir, au fil du temps, des pratiques pour la mise en place d'une surveillance de l'utilisation d'Internet au travail, pratiques qui sont, selon eux, raisonnables et fondées en droit. Il est par ailleurs légitime de se demander si, malgré ces croyances, les pratiques actuelles en matière de surveillance de l'utilisation d'Internet au travail respectent réellement les droits des personnes surveillées, particulièrement le droit à la vie privée des employés.

À titre d'exemple, une certaine croyance en matière de surveillance de l'utilisation d'Internet est à l'effet que si l'employeur adopte une politique de surveillance et la porte à la connaissance de ses employés, l'employeur peut dès lors exercer la surveillance. Selon cette croyance, l'existence de la politique et sa portée à la connaissance de l'employé ferait disparaître toute expectative de vie privée chez l'employé.

Or, est-ce que l'adoption d'une politique suffit pour permettre à l'employeur de surveiller toutes les activités Internet de ses employés au travail et ce, dans toutes les circonstances? N'y a-t-il pas des limites à respecter, limites étant imposées par les droits des employés? Est-ce que le simple fait que l'employé soit informé de la surveillance fait en sorte que ce dernier ne dispose plus d'une expectative raisonnable de vie privée à l'égard des activités Internet surveillées? Pouvons-nous réellement croire que l'expectative raisonnable de vie privée dépend uniquement de la décision de l'employeur de soumettre ou non ses employés à une surveillance?

Une autre croyance est à l'effet qu'étant donné que les outils informatiques appartiennent à l'employeur et sont fournis à des fins professionnelles, l'employeur a

le droit de surveiller l'utilisation qui en est faite par ses employés.

Or, est-ce le simple droit de propriété de l'employeur à l'égard des outils informatique fait disparaître le droit à la vie privée de l'employé? N'y a-t-il pas des décisions québécoises qui ont affirmé que l'employé disposait d'une expectative de vie privée dans le contexte de l'utilisation du téléphone au travail, et ce même si le téléphone appartient à l'employeur? Qu'est-ce qui nous permet de considérer le contraire en matière d'utilisation d'Internet au travail?

Les pratiques et croyances établies en matière de surveillance de l'utilisation d'Internet au travail suscitent de sérieux doutes quant à leur fondement et quant à leur justification en vertu du droit québécois.

Par ailleurs, plusieurs questions soulevées demeurent actuellement sans réponse, notamment les questions suivantes : (i) est-ce que l'employé dispose d'une expectative raisonnable de vie privée dans le cadre de l'utilisation d'Internet au travail?; (ii) quels sont les facteurs qui ont pour effet d'augmenter ou de réduire l'expectative raisonnable de vie privée d'un employé dans le cadre de l'utilisation d'Internet au travail?; (iii) est-ce que l'utilisation d'Internet au travail se compare à l'utilisation du téléphone, du courrier postal, ou d'un casier personnel sur le lieu de travail?; (iv) est-ce que l'employeur a des obligations en matière de protection des renseignements personnels lors de la mise en place d'une telle surveillance?; (v) est-ce que les employés doivent invoquer leur droit à la vie privée ou leur droit à des conditions de travail justes et raisonnables à l'encontre de l'exercice de la surveillance de l'utilisation d'Internet au travail?; (vi) quels sont les critères du droit de surveillance?; (vii) quels sont les obligations préalables à l'exercice de la surveillance?; (viii) quelles sont les exceptions à ces obligations?; et (ix) est-ce que l'employeur a des obligations vis-à-vis des tiers dans le cadre de la surveillance?

Notre objectif est non seulement de fournir une réponse à toutes ces questions, mais plus spécifiquement de fournir aux employeurs et à leurs conseillers juridiques un guide juridique pratique pour la mise en place une surveillance de l'utilisation

d'Internet au travail. Pour éviter que les employeurs exercent une telle surveillance en portant atteinte aux droits des employés ou des tiers, il est essentiel que les employeurs aient à leur disposition un énoncé clair de leurs droits et obligations lors de la mise en place de la surveillance. Nous exposerons donc les différents droits et obligations des personnes impliquées dans le contexte d'une surveillance de l'utilisation d'Internet au travail, ainsi que les étapes à suivre pour atteindre un équilibre entre les différents intérêts en jeu.

Tant les employeurs des organismes privés que des organismes publics québécois pourront tirer profit du présent mémoire et ce, indépendamment du fait que la surveillance soit déjà mise en place ou qu'elle constitue un projet futur. Par ailleurs, le lecteur pourra prendre note que nous utiliserons le terme « entreprise » pour désigner tant les organismes privés que publics.

Notre exposé se limite au cadre légal de la mise en place de la surveillance, c'est-à-dire aux facteurs et critères à prendre en considération lors de l'instauration, au sein d'une entreprise, d'un système de surveillance de l'utilisation d'Internet des employés. Les employeurs pourrons alors bâtir la surveillance sur une base solide de manière à éviter les contestations de la part du syndicat ou des employés, ou encore l'irrecevabilité en preuve des résultats obtenus dans le cadre de la surveillance. Le lecteur doit bien comprendre nous ne traiterons pas de la conservation, de la communication, de l'accès ou de la destruction des résultats de la surveillance, lesquels pourraient à eux seul faire l'objet d'un mémoire distinct.

Nous avons divisé le mémoire en trois chapitres portant respectivement sur la mise en contexte de la surveillance, les intérêts en jeu, et les critères et obligations à respecter lors de la mise en place de la surveillance.

Le premier chapitre met le lecteur en contexte relativement à la surveillance de l'utilisation d'Internet au travail. Pour être en mesure d'établir les principes applicables en matière de surveillance de l'utilisation d'Internet au travail, il est essentiel de bien comprendre d'où provient ce besoin de vouloir surveiller les

activités Internet de ses employés et quelles sont les raisons qui peuvent pousser un employeur à vouloir surveiller les activités Internet de ses employés. Le lecteur pourra constater que l'exercice d'une telle surveillance n'est pas toujours le caprice d'un employeur curieux et désireux de vouloir épier les activités Internet de ses employés sans raison légitime.

Bien que l'utilisation d'Internet au travail offre plusieurs effets bénéfiques pour un employeur, cette utilisation expose en contrepartie l'employeur à de nombreux risques, tant techniques que juridiques. Chacun de ces risques est exposé en détails dans le premier chapitre et est illustré à l'aide d'exemples tirés de la jurisprudence tant québécoise, canadienne, qu'américaine. À la lumière de ces nombreux exemples, le lecteur pourra constater que l'employeur a non seulement de nombreuses raisons, mais également de sérieuses raisons de vouloir éliminer ou réduire ces risques, et que la surveillance de l'utilisation d'Internet au travail constitue un bon outil pour atteindre cet objectif.

Par ailleurs, afin d'être en mesure d'évaluer l'impact d'une surveillance sur les droits des personnes surveillées, il est nécessaire de connaître les différents types de surveillance de l'utilisation d'Internet qui peuvent être exercés par l'employeur. En effet, l'employeur qui entend surveiller l'utilisation d'Internet au travail dispose de plusieurs options, tant au niveau de l'étendue de la surveillance, du type de surveillance exercée que de l'intensité de la surveillance. La fin du premier chapitre sera donc réservée à la description des différentes options offertes à l'employeur dans le cadre de la surveillance de l'utilisation d'Internet au travail.

Le deuxième chapitre expose au lecteur les enjeux juridiques de la surveillance. Comme tout problème juridique, la surveillance de l'utilisation d'Internet met en cause des intérêts concurrents. La mise en place d'une surveillance de l'utilisation d'Internet au travail requiert l'atteinte et le maintien d'un équilibre entre d'un côté les droits de l'employeur, plus particulièrement son pouvoir de direction et de contrôle, et de l'autre côté les droits des employés et des tiers, plus particulièrement leur droit à la vie privée et à des conditions de travail justes et raisonnables. Chacun de ces droits

est analysé en profondeur dans le deuxième chapitre.

Dans le cadre de l'analyse des différents intérêts en jeu, nous verrons notamment si, en vertu du droit québécois, l'employeur peut invoquer son droit de propriété afin de justifier l'exercice d'une surveillance de l'utilisation d'Internet au travail. Nous verrons également quels sont les facteurs à prendre en considération afin de déterminer si un employé dispose d'une expectative raisonnable de vie privée dans l'utilisation d'Internet au travail. Nous verrons par ailleurs l'impact de l'adoption d'une politique de surveillance, ou encore de l'obtention d'un consentement à l'égard de la surveillance, sur le droit à la vie privée de l'employé au travail. Et nous verrons que les tiers qui communiquent avec les employés peuvent également faire valoir des droits à l'encontre de l'exercice d'une surveillance de l'utilisation d'Internet au travail.

Finalement, le troisième chapitre se veut un guide pratique pour la mise en place d'une surveillance de l'utilisation d'Internet au travail. Il expose les critères et obligations à respecter pour que la surveillance de l'utilisation d'Internet au travail ne porte pas indûment atteinte aux droits des employés ou des tiers. À l'aide d'analogies tirées des principes applicables en matière de surveillance vidéo, d'écoute téléphonique ou de fouille au travail, nous verrons que l'employeur doit respecter certains critères lorsqu'il met en place une surveillance de l'utilisation d'Internet. Dans certains cas, l'employeur doit s'assurer d'informer ses employés de l'existence de la surveillance et d'obtenir leur consentement à cet égard. Dans d'autres situations, l'existence de circonstances particulières permet à l'employeur de se soustraire à ces obligations. Tout dépend du poids que prennent les différents intérêts en jeu, à la lumière de l'analyse des principes établis au deuxième chapitre. Par ailleurs, une liste de vérification sous forme de tableaux complète ce chapitre et regroupe les différentes étapes de réflexion que doit suivre l'employeur qui désire instaurer une surveillance de l'utilisation d'Internet au travail.

1. MISE EN CONTEXTE DE LA SURVEILLANCE DE L'UTILISATION D'INTERNET AU TRAVAIL

1.1. Un bref aperçu de la réalité

La présence d'Internet au travail est désormais incontournable. En 2007, 87% des entreprises canadiennes privées utilisaient Internet dans le cadre de leurs affaires et 81% utilisaient le courrier électronique[2]. Internet étant de plus en plus présent au sein des entreprises, le nombre d'employés ayant un accès direct à Internet à partir de leur travail a augmenté au fil des ans[3], ayant atteint un seuil de 62% de la population active du Québec en 2007[4].

Les principaux utilisateurs d'Internet en milieu de travail sont les personnes

---

[2] STATISTIQUE CANADA, « Commerce électronique et technologie », *Le Quotidien*, 24 avril 2008, en ligne : http://www.statcan.gc.ca/daily-quotidien/080424/dq080424a-fra.htm. Au niveau des PME québécoises, voir : CEFRIO, *NetQuébec 2008 – Portrait de l'utilisation des TI et d'Internet au Québec*, Montréal, 2008, en ligne : http://cefrio.qc.ca/fckupload/DEPL_netQuébec_web_SECUR.pdf.

[3] Sabrina CÔTÉ, *NETendances 2007, Évolution de l'utilisation d'Internet au Québec depuis 1999*, version abrégée, Montréal, CEFRIO, 2007. Selon cette étude, le pourcentage des québécois ayant accès à Internet, incluant le courrier électronique, dans le cadre de leur travail a évolué comme suit : 29.9% (2001), 32.8% (2002), 31.9% (2003), 41.4% (2004), 42.3% (2005), 47% (2006), et 47% (2007). Au Canada, voir : STATISTIQUE CANADA, *Enquête canadienne sur l'utilisation d'Internet, utilisation d'Internet, selon le point d'accès, le sexe et le groupe d'âge, aux 2 ans (pourcentage), 2005 à 2007*, CANSIM : tableau 358-0124.

[4] S. CÔTÉ, préc., note 3, p. 55. Voir également : Caroline BEAUDOIN, « Les travailleurs québécois considèrent que l'accès à Internet augmente la productivité », dans *Fiche de renseignements des Services Kelly – Résultats du sondage Internet – Canada*, 26 mars 2007, en ligne : http://www.kellyservices.ca/res/content/ca/services/fr/docs/Québec_internet_release_final_french.pdf. Au Canada, voir : STATISTIQUE CANADA, « Commerce électronique et technologie », préc., note 2. Aux États-Unis, voir : HARRIS INTERACTIVE, *Websense, Inc. Web@Work Survey 2006*, New York (États-Unis), mai 2006, en ligne: http://www.websense.com/global/en/PressRoom/MediaCenter/Research/webatwork/Employee_Computing.pdf; et BUREAU OF LABOUR STATISTICS, *Computer and Internet Use at Work in 2003*, United States Department of Labor, Octobre 2003, en ligne: http://www.bls.gov/news.release/pdf/ciuaw.pdf. En France, voir : ISEE, « Des TIC de plus en plus diversifiées dans les entreprises », dans *INSEE Première*, no. 1126, France, Mars 2007; et SERVICE DES ÉTUDES ET DES STATISTIQUES INDUSTRIELLES (SESSI), DiGITIP, « L'utilisation des TIC dans les entreprises », dans *Le 4 Pages des statistiques industrielles*, No. 201, France, janvier 2005.

diplômées de l'université (73.3%)[5]. Au niveau de l'âge, les 25-44 ans (64%) sont les plus grands utilisateurs, et au niveau du sexe, ce sont les hommes (51.4%) qui surpassent les femmes (41.9%)[6].

Le fait que de plus en plus d'employés disposent de l'accès à Internet dans le cadre de leur travail illustre les avantages qu'apporte l'intégration des nouvelles technologies de l'information et de la communication au sein des entreprises. Par ailleurs, afin de bien évaluer les bénéfices apportés par l'utilisation d'Internet en milieu de travail, il est nécessaire de connaître l'étendue de l'utilisation d'Internet et le type d'utilisation qui en est faite par les employés.

À cet égard, les données de NETendances indiquent que les travailleurs québécois qui disposent d'un accès à Internet à leur travail passent en moyenne sept heures et demie par semaine, soit environ 20% de leur semaine de travail, à naviguer sur le net, que ce soit pour des fins personnelles ou professionnelles, pour surfer sur le net ou pour communiquer par courriel[7].

L'étendue grandissante de l'utilisation d'Internet au travail comporte autant d'avantages que d'inconvénients pour les employeurs qui décident de fournir un accès à Internet à leurs employés. Ces avantages et inconvénients peuvent, au moyen de la surveillance, être soit maximisés soit diminués, de façon à en tirer le maximum de bénéfice. Voyons maintenant en détail ces différents risques et avantages.

1.2. Les avantages liés à l'utilisation d'Internet au travail

1.2.1. Généralités

---

5 Sabrina CÔTÉ, *NETendances 2007, Évolution de l'utilisation d'Internet au Québec depuis 1999*, version intégrale, Montréal, CEFRIO, 2007, p. 56.

6 *Id.*

7 Éric LACROIX, *NETendances 2002, Utilisation d'Internet au Québec,* version abrégée, Montréal, CEFRIO, Janvier 2003 (cette donnée ne se retrouve pas dans les rapports publiés par NETendances depuis 2002). Aux États-Unis, voir : HARRIS INTERACTIVE, préc., note 4, qui indique une moyenne de 10,2 heures d'utilisation par semaine.

La décision pour un employeur de fournir un accès à Internet à ses employés découle généralement des avantages que peut lui procurer l'utilisation de certains services et outils Internet. Afin d'augmenter ses profits, une entreprise a intérêt à doter ses employés de ressources efficaces, complètes et rapides, de façon à améliorer sa productivité, tout en réduisant les coûts de production et de fourniture de services. D'ailleurs, selon une étude effectuée en 2007[8], 65% de la population active québécoise considère que l'accès au courrier électronique et à Internet améliore leur productivité. De plus, avec la mondialisation croissante des marchés et l'utilisation grandissante des technologies de l'information et de la communication au sein des entreprises, les entreprises doivent indéniablement être connectées à Internet si elles veulent demeurer compétitives sur le marché.

Les avantages liés à l'utilisation d'Internet au travail touchent à deux facteurs déterminants pour la productivité d'une entreprise : i) les communications internes et externes des employés; et ii) l'information à laquelle les employés ont accès dans le cadre de leur travail.

1.2.2. Les communications

À l'égard des communications, les entreprises sont constamment à la recherche de réactivité et de prises de décisions rapides. Les personnes travaillent de plus en plus en collaboration, que ce soit à l'intérieur de l'entreprise ou avec des partenaires extérieurs, et les exigences de présence et de disponibilité vis-à-vis de ces personnes prennent une importance croissante. Il importe d'être en mesure de rejoindre rapidement les personnes avec qui elles sont en affaires et de demeurer disponibles pour répondre rapidement à leurs demandes en cas de besoin. Dans ce contexte, les technologies, particulièrement les communications Internet, se développent rapidement afin de pouvoir répondre à ces exigences des entreprises.

Internet offre actuellement plusieurs outils pour faciliter les communications internes

---

[8] C. BEAUDOIN, préc., note 4.

ou externes des employés, et ainsi permettre aux entreprises d'optimiser leur productivité. Il s'agit plus particulièrement du courrier électronique, de la messagerie instantanée et des blogs. Voici maintenant un bref aperçu de l'étendue et des avantages que procure l'utilisation de ces trois outils.

1.2.2.1. Le courrier électronique

Dans la plupart des entreprises, le courrier électronique (également appelé « courriel », « mél », « e-mail » ou « email ») est devenu le moyen usuel de communication, tant pour des fins de discussion que pour la transmission d'information. En 2007, 81% des entreprises canadiennes du secteur privé et 100% des entreprises canadiennes du secteur public utilisaient le courrier électronique dans le cadre de leurs affaires[9].

La popularité de ce moyen de communication n'est pas surprenante si l'on pense aux avantages qu'offre le courrier électronique par rapport aux médiums traditionnels. Cet outil permet à l'utilisateur d'envoyer des messages instantanément à n'importe qui disposant d'un accès à Internet, et ce, n'importe où et à faible coût. Il est donc aussi facile de communiquer avec une personne située dans la pièce d'à côté qu'avec une personne située à l'autre bout de la planète. Par ailleurs, transmettre un courriel ou y répondre est facile, simple, et n'est pas restreint à l'obligation de devoir se connecter avec une personne en « temps réel », comme c'est le cas avec le téléphone. La réception des messages est par ailleurs beaucoup plus rapide que le courrier postal. Dépendamment de la connexion Internet et du volume du message, ce dernier arrivera à destination au même rythme que le message est transmis, plutôt qu'une seule fois par jour.

De plus, le courrier électronique permet non seulement de transmettre un message textuel, mais également d'y joindre des fichiers de différents formats et de différents volumes tels que des documents textes, des instructions, des fichiers audio ou vidéo,

---

[9] STATISTIQUE CANADA, « Commerce électronique et technologie », préc., note 2.

permettant ainsi de réduire le coût et le temps de transmission lorsque l'on fait affaires avec des personnes situées à l'extérieur de la ville ou du pays.

Finalement, les traces laissées par l'envoi et la réception de messages dans la boîte de courrier électronique ou dans l'ordinateur de l'utilisateur assurent un suivi facile et rapide des communications. Il n'est plus nécessaire de noter les communications effectuées, compte tenu que l'historique complet des messages se trouve automatiquement[10] dans la boîte de courrier électronique de l'utilisateur.

Le courrier électronique constitue donc un excellent moyen pour l'entreprise d'accroître la rapidité et l'efficacité des communications de ses employés tant avec ses fournisseurs, ses clients ou ses partenaires, et que ce soit pour des fins de promotion, de coordination, ou de consultation, pour accroître sa visibilité ou pour atteindre une clientèle à plus grande échelle[11].

1.2.2.2. La messagerie instantanée

La messagerie instantanée est un deuxième outil de communication Internet de plus en plus utilisé en milieu de travail, allant même jusqu'à remplacer progressivement le courrier électronique comme outil de communication[12]. La messagerie instantanée (également appelé « clavardage » ou « *chat* ») est une « activité permettant à une personne d'avoir une conversation écrite, interactive et en temps réel avec une ou plusieurs personnes connectées simultanément au réseau Internet, par claviers interposés »[13]. En se connectant au même moment à des serveurs par le biais de logiciels de messagerie instantanée, les utilisateurs peuvent communiquer entre eux

---

[10] Cette fonction dépend des logiciels de courrier électronique mais, en principe, les boîtes de courrier électronique fournissent l'option de sauvegarder les messages envoyés et reçus.

[11] À l'égard des avantages perçus par les entreprises privées canadiennes de faire affaires sur Internet, voir : STATISTIQUE CANADA, « Commerce électronique et technologie », préc., note 2, qui indique les avantages suivants : (i) réduction des coûts (30%); élargissement de la clientèle (36%); meilleure coordination avec les fournisseurs, clients et partenaires (36 %); et réduction du temps nécessaires à commercialiser (19%).

[12] Nancy FLYNN, *Instant Messaging Rules*, New York, AMACOM, 2004, p. 8.

[13] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE (OQLF), « Le grand dictionnaire terminologique », en ligne : http://www.granddictionnaire.com.

instantanément et s'échanger toutes sortes d'informations sous différents formats.

Les données de NETendances 2007[14] révèlent que 17,9% de la population québécoise utilise la messagerie instantanée à partir de son travail. Cette proportion grimpe à 39% si l'on se réfère uniquement à la population active québécoise qui utilise Internet au travail, et à 26,1% si l'on se réfère aux adultes québécois qui occupent un emploi. Par ailleurs, selon une étude de la compagnie Gartner[15], d'ici 2010, la proportion des travailleurs québécois qui utilisent le courrier électronique qui auront aussi un compte de messagerie instantanée au travail grimpera à 90%.

La popularité croissante de cet outil n'est pas étonnante compte tenu de sa rapidité qui la rend dans bien des cas plus efficace que le courrier électronique. Un de ses principaux avantages pour le moins non négligeable est l'instantanéité des conversations ou de la diffusion d'information. Envoyer un courrier électronique à un interlocuteur implique nécessairement un délai de réponse, compte tenu que le message s'ajoute à tous les autres messages reçus par l'interlocuteur. Par contre, transmettre un message par messagerie instantanée ajoute un caractère prioritaire au message, lequel nécessite une réponse immédiate. Cet avantage est d'ailleurs l'une des raisons qui ont mené à l'intégration de la messagerie instantanée dans les téléphones mobiles, notamment MIMAIL de Comverse, de l'utilisation grandissante des Blackberry[16], iPhone ou technologies similaires, de même qu'au développement et à la mise en marché de nombreux logiciels de messagerie instantanée destinés aux entreprises, tels que Instant messenger for LAN de Softros Systems, Inc., e/Pop, Microsoft enterprise IM client, Hummingbird Enterprise IM, OpenScape Mobility de

---

[14] S. CÔTÉ, version abrégée, préc., note 3, p. 56. Aux États-Unis, voir : AMERICAN MANAGEMENT ASSOCIATION (AMA) AND THE EPOLICY INSTITUTE, *2006 Workplace E-Mail, Instant Messaging & Blog Survey*, États-Unis, 2006, en ligne : http://www.epolicyinstitute.com/survey2006Summary.pdf, qui indique un pourcentage de 35% en 2006.

[15] Matthew W. CAIN, David Mario SMITH, and Betsy BURTON, « Management update : wake up to the realities of instant messaging », October 19, 2005, Gartner Inc. (Research : G00133673), en ligne : http://www3.villanova.edu/gartner/research/133600/133673/133673.pdf.

[16] La technologie *BlackBerry* permet de recevoir et envoyer des courriels et de se brancher à Internet via un terminal mobile de poche.

Siemens, Softros LAN Messenger et l'application iPhone OneTeam.

1.2.2.3. Les blogs

Un troisième outil Internet de plus en plus utilisé dans les entreprises est le blog. Un blog est un site ou encore un ensemble de pages web sur lequel l'auteur ou les personnes autorisées à y participer s'expriment sous la forme de billets ou d'articles informatifs à la manière d'un journal de bord. Les billets ou articles sont parfois enrichis d'hyperliens, d'images, de sons (ex. radioblogues) et de vidéos (ex. vidéo blogues), et peuvent faire l'objet de commentaires de la part des lecteurs, lesquels sont ensuite publiés et rendus disponibles pour les autres lecteurs.

Les blogs d'entreprises peuvent être réservés à la communication interne entre les employés ou encore être publics et permettre la communication avec la clientèle ou des tierces personnes. Certains employeurs vont inciter leurs employés à participer au blog d'entreprises, alors que d'autres vont réserver la gestion du blog à des personnes précises au sein de l'entreprise. En 2006, 8% des entreprises américaines opéraient un blog d'entreprise et 50% de ces blogs étaient publics[17].

Les blogs offrent de nombreux avantages pour les entreprises, notamment la possibilité de publier de l'information sans devoir passer par un intermédiaire, sans avoir à diffuser un communiqué de presse ou un bulletin d'information. Ils offrent également une opportunité de discussion directe avec les clients, lesquels peuvent donner leur avis sur les produits et services, ou encore communiquer rapidement les problèmes survenus dans le cadre de leur utilisation. De plus, grâce maintenant aux fils d'information (par exemple RSS[18]), les lecteurs peuvent maintenant être rapidement informés des mises à jour du blog.

---

[17] AMERICAN MANAGEMENT ASSOCIATION (AMA) AND THE EPOLICY INSTITUTE, préc., note 14.

[18] WIKIPEDIA, « RSS (Format) », 2009 : « Le format RSS désigne une famille de formats XML utilisés pour la syndication de contenu Web. Ce système est habituellement utilisé pour diffuser les mises à jour de sites dont le contenu change fréquemment, typiquement les sites d'information ou les blogs. L'utilisateur peut s'abonner aux flux, ce qui lui permet de consulter rapidement les dernières mises à jour sans avoir à se rendre sur le site », en ligne : http://fr.wikipedia.org/wiki/RSS_(format).

Par ailleurs, plusieurs collaborateurs parlent de leur entreprise sur leurs propres blogs, donnant ainsi une toute autre image de l'entreprise que celle qui apparaît dans les rapports annuels, les sites institutionnels et les communiqués de presse[19]. Certaines entreprises voient cette tendance d'un bon œil, considérant que les blogs humanisent l'entreprise vers l'extérieur, et offrent aux employés et aux groupes de travail la possibilité de discuter de certains produits et services avec une plus large communauté d'experts en technologies. À titre d'exemple, les blogs de Microsoft permettent aux employés et aux groupes de travail de l'entreprise de discuter des produits et services offerts sur le marché par Microsoft, avec une large communauté de professionnels, spécialistes ou amateurs, de façon à améliorer le développement et le déploiement de leurs produits et services[20].

1.2.3. Les sources d'information

1.2.3.1. Le World Wide Web

Internet n'offre pas seulement des outils de communication; il offre également d'importants outils de recherche et de consultation. En effet, le World Wide Web (WWW, « le Web » ou « la Toile »), qui constitue l'espace du réseau sur lequel sont proposés des pages de texte, des graphiques voire du son ou des clips vidéo, donne accès à une véritable bibliothèque numérique, à d'innombrables pages web et bases de données de nature scientifique, financière, commerciale, culturelle, journalistique ou humoristique. Ces pages peuvent être publiées par toute personne disposant d'un accès à l'espace de stockage sur un ordinateur « hôte » relié à Internet moyennant le logiciel approprié (un « serveur Web » ou « site »). Avec l'utilisation des moteurs de recherches disponibles, la navigation sur le Web peut se révéler un outil très efficace pour obtenir des informations sur différents sujets.

---

[19] Loic LE MEUR, « Les webblogs et leur utilisation en interne pour les entreprises », dans *Six Apart SA*, France, 2006, en ligne : http://loiclemeur.com/english/images/KM_loic2.pdf.

[20] Voir la rubrique des Bloggeurs de Microsoft France, à l'adresse URL suivante : http://www.microsoft.com/france/blogs/blogs.mspx.

La prolifération des informations disponibles sur le réseau Internet connaît une croissance marquée, liée notamment au phénomène du contenu généré par les utilisateurs (« *user generated content* ») et du journalisme citoyen. Les utilisateurs d'Internet jouent de plus en plus un rôle actif quant à l'information et au contenu rendus disponibles sur le réseau. Plutôt que d'être uniquement récepteurs de l'information, les utilisateurs deviennent maintenant des émetteurs. Plusieurs documents de recherche et d'articles de toutes sortes sont diffusés sur le réseau directement par leur auteur et de nombreux forums de discussion ou blogs permettent aux internautes d'échanger des informations et des commentaires sur des sujets variés. Grâce à ce phénomène, les employés peuvent facilement se tenir à jour sur des sujets d'actualité qui touchent leur domaine d'emploi.

À la lumière de ce qui précède, Internet est sans contredit un outil dont les entreprises peuvent maintenant difficilement se passer. Internet permet d'augmenter la productivité d'une entreprise, lui offre une meilleure visibilité sur le marché et lui permet d'améliorer ses relations avec ses clients ou partenaires d'affaires. Néanmoins, toute bonne chose comporte également un revers dont il faut se méfier. Nous allons donc maintenant exposer les risques liés à l'utilisation d'Internet au travail.

1.3. Les risques engendrés par l'utilisation d'Internet par les employés

1.3.1. Généralités

Tant l'usage du courrier électronique, la navigation sur le Web, le téléchargement de fichiers ou la diffusion de contenu sur le Web peuvent avoir un effet dévastateur sur l'entreprise, que ce soit au niveau de son image, de la protection de ses informations confidentielles, de la sécurité de ses données, de sa responsabilité juridique ou des pertes financières. Ces risques peuvent varier en fonction du type d'entreprise, du type de travail effectué par chacun des employés et du type de service ou d'outil Internet utilisé, mais les employeurs qui fournissent un accès à Internet à leurs employés doivent prendre conscience de l'existence et de l'étendue de ces risques afin d'être en mesure de les éviter ou de les réduire.

Par ailleurs, Internet comporte des risques même si son utilisation est faite à des fins professionnelles. Bien que ces risques puissent être réduits en interdisant certains types d'utilisations, plusieurs d'entre eux sont inhérents à l'utilisation du réseau et demeurent présents indépendamment des fins pour lesquelles ils sont utilisés. Par exemple, l'utilisation du courrier électronique comporte en tout temps le risque que le système informatique soit affecté par un virus électronique, que le message soit transmis à des fins personnelles ou professionnelles.

Dans la présente section, nous exposerons les risques liés à l'utilisation d'Internet en les divisant en deux catégories, soit les risques techniques liés au bon fonctionnement du réseau et les risques juridiques liés à la responsabilité de l'entreprise, au vol de temps, à la loyauté des employés et à la protection des renseignements confidentiels de l'entreprise.

1.3.2. Les risques techniques

1.3.2.1. L'encombrement du réseau

Afin d'optimiser l'utilisation d'Internet, il est important que la connexion à Internet et la vitesse de transmission soient la plus élevée possible, de façon à ce que les employés puissent rapidement avoir accès aux informations transmises sur le réseau. La performance de la connexion et de la transmission des données dépend du débit de la connexion. Le débit d'une connexion est la quantité de données transmise pendant une unité de temps. On l'exprime en bits par secondes, bit/s (le bit étant la quantité élémentaire d'information numérique, un 0 ou un 1), ou encore en octets (8 bits) par seconde. Le débit est lié à l'infrastructure du réseau : il est limité par la rapidité des équipements actifs, tels que les routeurs et les modems, et par la nature des supports physiques de transmission, tels que des fils de cuivre ou la fibre optique.

La vitesse de transmission d'un message ou d'un fichier, qui correspond en fait à la quantité totale d'information transmise par le support physique par seconde (ex. 54Mb/s), variera dépendamment de l'encombrement du réseau et du nombre de personnes connectées simultanément aux sites visités. Par conséquent, si un employé

télécharge un fichier trop lourd ou de taille excessive à partir d'Internet, cela risque de ralentir ou de paralyser le réseau de la compagnie.

La bande passante utilisée par les employés sera d'autant plus grande si les employés utilisent Internet à des fins personnelles et non uniquement dans le cadre de leur travail. Le ralentissement du réseau causé par des mauvais usages ou des usages inutiles peut occasionner des pertes de temps et d'argent inutiles pour l'entreprise. En plus du ralentissement du temps de réponse sur le réseau, l'entreprise se verra débourser des frais pour que son réseau puisse répondre adéquatement aux demandes croissantes d'accès Internet.

1.3.2.2. La sécurité du réseau

Par ailleurs, l'une des principales préoccupations des entreprises qui disposent d'un accès à Internet concerne la sécurité du réseau de l'entreprise. Celle-ci peut être mise en danger tant par une mauvaise utilisation du réseau informatique que par des attaques extérieures telles que des virus informatiques, des vers, des chevaux de Troie, ou des logiciels espions.

Un virus informatique se définit de la façon suivante :

> « Programme malveillant dont l'exécution est déclenchée lorsque le vecteur auquel il a été attaché clandestinement est activé, qui se recopie au sein d'autres programmes ou sur des zones systèmes lui servant à leur tour de moyen de propagation, et qui produit les actions malveillantes pour lesquelles il a été conçu. »[21]

Quant au ver, il s'agit d'un programme qui crée et distribue des copies de lui-même. Il est conçu pour se répliquer d'ordinateur en ordinateur mais contrairement au virus, il le fait de façon autonome en prenant le contrôle de certaines fonctionnalités capables de transporter des fichiers ou des informations. Il n'a pas besoin d'un programme ou d'un fichier « hôte » pour se propager. Un ver pourra donc envoyer des copies de lui-même à tous les destinataires du carnet d'adresses de courrier

---

[21] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE (OQLF), « Le grand dictionnaire terminologique », en ligne : http://www.granddictionnaire.com.

électronique. Les ordinateurs de ces destinataires feront de même, ce qui créera un effet de cascade et générera une surcharge de trafic tellement importante qu'elle ralentira les réseaux des entreprises et d'Internet dans son ensemble. Les vers peuvent également ouvrir une brèche dans le système de l'ordinateur et permettre à un intrus d'en prendre le contrôle à distance.

Un cheval de Troie va attaquer d'une manière bien différente. Il va dissimuler son identité et ses activités jusqu'à son exécution. Contrairement au virus et au ver, le cheval de Troie ne se reproduit et ne se copie pas. Il peut être envoyé par une tierce personne ou encore véhiculé par un autre programme, sous la forme d'un programme informatique d'apparence utile, mais conçu en réalité pour causer des dommages. Les chevaux de Troie se propagent donc en amenant les utilisateurs à ouvrir un programme qu'ils pensent issus d'une source digne de confiance.

Finalement, un logiciel espion (en anglais *spyware*) couvre tout « logiciel qui contient un programme espion et qui emploie en arrière-plan la connexion Internet de l'utilisateur pour recueillir et transmettre, à son insu et sans sa permission, des données personnelles, notamment sur ses intérêts et ses habitudes de navigation, à une régie publicitaire »[22].

Tous ces programmes malveillants attaquent généralement par le biais des données qui entrent dans le réseau. Ces attaques peuvent causer des vols, des pertes de données, ralentir la connexion Internet, contaminer le réseau informatique de personnes et même causer une interruption complète du réseau de l'entreprise. Ces attaques se font généralement par le transfert de fichiers par courrier électronique, messagerie instantanée ou par les réseaux poste-à-poste[23].

---

[22] *Id.*

[23] Le terme « poste-à-poste » (ou en anglais « *peer-to-peer* ») se définit comme étant « un dispositif technique permettant l'échange de fichiers entre internautes, à travers le réseau Internet » : Pierre ALCATRAZ, *La notion de copie privée*, Mémoire de D.E.A. de Propriété intellectuelle, Nantes, Faculté de Droit et de Sciences politiques, Université de Nantes, 2002-2003, p. 26.

Un sondage américain effectué en 2008[24] révèle que 50% des entreprises américaines ont été victimes d'une attaque par virus ou autre type de programme malveillant, 44% auraient souffert d'une mauvaise utilisation du système informatique par leurs employés, 29% auraient fait l'objet d'intrusions extérieures non-autorisées et 5% auraient souffert de vol ou de fraude informatique.

Les conséquences d'une attaque informatique peuvent être majeures. Non seulement la réparation du système informatique peut prendre du temps et de l'argent, mais la perte d'informations peut avoir des conséquences financières importantes pour l'entreprise. Selon le sondage américain de 2008[25], les pertes annuelles subies par les entreprises américaines en 2008 suite à un bris de sécurité informatique sont en moyenne de 288 618,00 dollars américains.

1.3.3. Les risques juridiques

1.3.3.1. Généralités

L'utilisation d'Internet ne comporte pas uniquement des risques techniques. Les employeurs ont des droits et des obligations tant vis-à-vis l'entreprise, les clients, les employés et le public, lesquels entrent directement en ligne de compte lorsque les employés utilisent Internet au travail. L'employeur est en quelque sorte redevable des actes commis par ses employés dans le cadre de leurs fonctions. Sa responsabilité risque donc d'être engagée en fonction des activités auxquelles se livrent les employés sur Internet. De plus, certains employés ne sont pas aussi loyaux qu'ils le devraient. Certains peuvent tenter de nuire à l'employeur en publiant du contenu préjudiciable sur Internet, et d'autres abuser de l'utilisation d'Internet à des fins personnelles durant les heures de travail. Voici en détail les risques juridiques liés à l'utilisation d'Internet au travail.

---

[24] Robert RICHARDSON, « The 2008 CSI/FBI Computer Crime and Security Survey », États-Unis, en ligne : http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf, p. 15.

[25] *Id.*, p. 16.

1.3.3.2. La responsabilité de l'employeur en vertu du droit commun

1.3.3.2.1. LA RESPONSABILITÉ DES COMMETTANTS

En premier lieu, l'employeur peut voir sa responsabilité engagée à l'égard des tiers pour une utilisation illicite ou fautive d'Internet par ses employés. Cette responsabilité découle du régime de responsabilité des commettants tel que prévu à l'article 1463 C.c.Q.[26].

La mise en œuvre de ce régime de responsabilité ne requiert pas la commission d'une faute par l'employeur[27]. Dès que l'employé commet un geste fautif dans l'exécution de ses fonctions (dans ce cas-ci, ce serait dans le cadre de l'utilisation d'Internet au travail), son employeur devient automatiquement responsable des dommages qui en découlent. Les seules défenses possibles pour l'employeur sont : i) que les conditions mêmes de l'application du régime de responsabilité ne soient pas réunies; ii) qu'il s'agisse d'une force majeure; ou iii) que la victime ait elle-même commis une faute[28]. Par conséquent, même si l'employeur prouve qu'il a été diligent dans le choix de son employé, qu'il a exercé une surveillance adéquate quant aux actes de son employés sur le lieu de travail, qu'il a tout fait pour éviter ou pour prévenir le dommage ou encore que l'acte fautif était totalement imprévisible, sa responsabilité se verra engagée.

Néanmoins, il serait légitime de se demander si un employeur pourrait être tenu responsable des dommages causés par son employé dans le cadre d'une utilisation d'Internet, si cette utilisation est faite à des fins personnelles. Nous ne ferons pas ici une analyse exhaustive de la question, compte tenu que l'objet du présent chapitre est d'exposer les risques possibles de l'utilisation d'Internet. Toutefois, prenons

---

[26] C.c.Q, art. 1463 : « Le commettant est tenu de réparer le préjudice causé par la faute de ses préposés dans l'exécution de leurs fonctions; il conserve, néanmoins, ses recours contre eux. »

[27] Jean-Louis BEAUDOIN et Patrice DESLAURIERS, *La responsabilité civile*, 7e ed., vol. 1, Cowansville, Éditions Yvon Blais, 2007, n° 750, p. 714.

[28] *Id.*

l'exemple d'un employé qui publie un billet diffamatoire sur un blog n'ayant aucun lien avec son travail ou l'entreprise de l'employeur. Dans ce cas, l'activité effectuée sur Internet n'entre aucunement dans les fonctions de travail de l'employé. Si l'employeur prouve que l'utilisation fautive d'Internet s'est faite sans son autorisation, du fait par exemple qu'il avait mis en place une politique de l'utilisation d'Internet qui interdisait l'utilisation à des fins personnelles, nous pourrions prétendre que l'exercice des fonctions n'a été que l'occasion, le support ou le soutien fortuit de l'acte fautif, ayant facilité l'acte fautif, mais ne l'ayant pas directement provoqué[29].

Aucun tribunal québécois n'a encore eu à se pencher sur un litige impliquant la responsabilité de l'employeur dans le cas d'une utilisation fautive d'Internet[30]. Néanmoins, plusieurs jugements, notamment en France[31] et aux États-Unis[32], sont venus condamner des employeurs pour les fautes commises par leurs employés dans le cadre de l'utilisation d'Internet. Par conséquent, il s'agit d'un risque important et non négligeable que les employeurs doivent prendre en considération lorsqu'ils décident de fournir un accès à Internet à leurs employés. Nous exposerons maintenant les principaux actes fautifs pouvant être commis par les employés dans le cadre de l'utilisation d'Internet au travail.

1.3.3.2.1.1. *Le contenu préjudiciable ou illégal*

Internet offre de nombreux outils permettant à tous et chacun de s'exprimer sur des

---

[29] Par analogie avec les principes énoncés dans *Curley* c. *Latreille*, (C.S. Can., 1920-02-03), SOQUIJ AZ-50293164, 60 R.C.S. 131, 55 D.L.R. (2d) 461. En l'espèce, un chauffeur avait emprunté la voiture de son patron sans autorisation pour son propre plaisir. Voir également J.-L. BEAUDOIN et P. DESLAURIERS, préc., note 27, n° 850, p. 751 : « La responsabilité du commettant doit être exclue lorsque le comportement tend à l'obtention par le préposé d'un bénéfice exclusivement personnel, ou est uniquement en fonction de son intérêt propre ».

[30] En Alberta, voir l'affaire *Inform Cycle Ltd.* v. *Rebound Inc.*, (2006), [2007] 3 W.W.R. 556, 2006 ABQB 825, 2006 CarswellAlta 1578, 68 Alta. L.R. (4th) 185 (Alta. Master). En l'espèce, la Cour a conclu que l'employeur n'était pas responsable de l'acte de son employé.

[31] À titre d'illustration, voir : Trib. Gr. Inst. Marseille, 1e ch. Civ., 11 juin 2003, *SA Escota c/ Société Lycos, Société Lucent Technologies et M. N. B.*, conf. par CA Aix-en-Provence, 2e ch., 13 mars 2006, pourvoi no. 2006/170.

[32] À titre d'illustration, voir : *Marobie-FL, Inc.* v. *National Ass'n of Fire Equipment Disributors (NAFED)*, 983 F. Supp. 1167 (N.D. Ill. 1997).

sujets variés, que ce soit sur des sites personnels, des blogs ou des forums de discussion et malheureusement, cette multiplication des moyens d'expression multiplie également les dérapages au niveau du contenu publiés. À cet égard, une étude d'IBM Internet Security Systems (ISS) de 2008 évalue le pourcentage de contenu indésirable (incluant les sites de type pornographique, sexuel et criminel) à 8%[33]. En 2005, l'ISS avait d'ailleurs observé une augmentation de 42% du nombre de sites web dont le contenu présentait un caractère illégal ou extrémiste, faisant notamment l'apologie du racisme, de la pornographie, du suicide, du cannibalisme humain, du satanisme, ou fournissant des informations sur la façon de commettre des crimes ou des actes terroristes[34].

Il ne faut pas oublier que plusieurs droits fondamentaux tels que la protection des mineurs, la sécurité nationale, la protection de la dignité, de la vie privée et de la réputation des personnes, peuvent être grandement brimés si les contenus publiés sur Internet par les employés contiennent par exemple des informations fausses ou erronées[35], sont diffusées dans le but de nuire à autrui, donc diffamatoires[36] ou portent atteinte à la vie privée d'une autre personne[37]. Au Québec, il s'agit d'actes pouvant constituer des violations au *Code criminel du Canada*[38], à la *Charte canadienne des droits et libertés*[39], à la *Charte des droits et libertés de la personne*[40], et au *Code civil*

---

[33] IBM, *IBM Internet Security Systems – X-Force 2007 Trend & Risk Report*, États-Unis, IBM Global Technology Services, January 2009, en ligne : http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf.

[34] PARME COMMUNICATION ET INTERNET SECURITY SYSTEMS, *Le nombre de sites web aux contenus illégaux ou extrémistes a augmenté de 42% en 2005*, Communiqué de presse, France, 5 décembre 2005, en ligne : http://www.parmecommunication.com/outils/presse/read.php?page=116&client=18&message=467.

[35] *Bélisle (Maison Dutrisac)* c. *Association Les Naturalistes du Baptiste Lefebvre*, B.E. 2006BE-113 (C.Q.).

[36] Voir notamment *Investors Group c. Hudson*, [1999] R.J.Q. 599 (C.S.) (création d'un site web et diffusion de contenu diffamatoire sur le site web); et *Arpin* c. *Grenier*, [2004] R.J.D.T. 613, J.E. 2004-1172, (C.Q.) (publication d'un article à caractère offensant sur un forum de discussion avec l'utilisation de l'adresse électronique de l'employeur).

[37] Trib. Gr. Inst. Paris, 19 octobre 2006, *Mme H.P. c/ SARL Google France et Google Inc.*, n° RG 06/58312.

[38] L.R., 1985, ch. C-46. (ci-après « C.cr. »).

[39] Annexe B de la de la *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.) (ci-après « Charte canadienne »).

[40] L.R.Q., chapitre C-12 (ci-après « Charte Québécoise »).

du Québec[41].

En 2002, de nouvelles infractions ont d'ailleurs été créées dans le *Code criminel* afin d'adapter la loi aux nouveaux environnements électroniques[42]. Ainsi, il est maintenant expressément mentionné que le fait d'accéder en ligne à de la pornographie juvénile[43], de la transmettre ou de la rendre accessible[44], ou d'utiliser un ordinateur pour communiquer avec une personne que l'on croit être un enfant dans le but de faciliter la perpétration d'infractions sexuelles[45], sont des actes illégaux.

Compte tenu que dans toutes les situations impliquant un accès ou une publication de contenu préjudiciable ou illégal sur Internet l'employeur peut voir sa responsabilité engagée, ce dernier aura intérêt à exercer un certain contrôle ou une certaine surveillance au niveau de l'utilisation qui est faite des outils informatiques et de la connexion Internet par ses employés.

1.3.3.2.1.2. *La violation de la propriété intellectuelle*

L'utilisation d'Internet pose également des risques au niveau de la protection des droits de propriété intellectuelle[46], particulièrement au niveau des droits d'auteur. Au Canada, le droit d'auteur est protégé par la *Loi sur le droit d'auteur*[47]. Le titulaire du droit d'auteur a le droit exclusif de produire ou de reproduire son œuvre ou toute partie importante de son œuvre sous une forme matérielle quelconque, de la publier, de la performer en public, de la traduire, de la louer et de l'importer[48]. Si une personne

---

41 L.Q. 1991, c. 64 (ci-après« C.c.Q »).

42 Le Projet de loi C-15A, amendant le *Code criminel* et portant sur l'exploitation sexuelle des enfants sur Internet, a été sanctionné le 4 juin 2002.

43 C.cr. art. 163.1 (4.1) (accès à la pornographie juvénile).

44 C.cr. art. 163.1 (3) (distribution de pornographie juvénile).

45 C.cr. art. 172.1 (leurre des enfants).

46 Les droits de propriété intellectuelle couvrent les droits d'auteur, les brevets, les marques de commerce, les secrets de commerce et les dessins industriels.

47 L.R.C. 1985 ch. C-42 (ci-après « *Loi sur le droit d'auteur* »).

48 *Id.*, art. 3.

commet l'un de ces actes sans avoir préalablement obtenu l'autorisation du titulaire des droits d'auteurs, cela constitue une violation[49]. Et lorsque cette violation est commise par un employé dans le cadre de ses fonctions, l'employeur peut être tenu responsable de la violation à titre de commettant[50].

Par le biais d'Internet, il devient très facile de violer des droits sur des œuvres protégées, que ce soit intentionnellement ou par inadvertance.

En premier lieu, les droits de propriété intellectuelle peuvent être violés par du contenu contrefaisant. En effet, la reproduction non autorisée d'œuvres écrites, sonores ou d'images protégées, que ce soit sur un site Web, un blog, dans un forum de discussion ou dans les communications Internet, constitue une infraction. Est aussi interdite la reproduction ou l'utilisation d'un logo ou d'une marque commerciale déposée lorsqu'elle crée de la confusion dans l'esprit du public. À moins de bloquer le téléchargement de fichiers externes sur le poste de travail des employés, ceux-ci peuvent facilement télécharger toutes sortes de fichiers, qu'ils soient sous forme d'images, de textes, de logiciels ou de fichiers audio/vidéo, pour ensuite les distribuer à des tiers ou les intégrer dans leur travail, le tout sans avoir préalablement obtenu le consentement du titulaire des droits sur l'œuvre protégée.

Internet comporte par ailleurs des risques au niveau des logiciels utilisés par les employés dans le cadre de leur travail et de la possibilité pour les employés de télécharger des logiciels piratés à partir d'Internet. À cet égard, il est important de comprendre que le droit de faire une copie d'un programme informatique entre dans les droits exclusifs du titulaire des droits d'auteur de reproduire son œuvre[51]. Si l'employé utilise une copie piratée d'un logiciel, il utilise alors ce logiciel sans

---

[49] Il y a toutefois certaines exceptions au niveau de l'utilisation équitable (*Loi sur le droit d'auteur,* art. 29, 29.1 et 29.2).

[50] À titre d'illustration, voir : *Marobie-FL, Inc.* v. *National Ass'n of Fire Equipment Disributors.(NAFED)*, préc., note 32.

[51] L'article 30.6 *Loi sur le droit d'auteur* prévoit néanmoins deux exceptions à ce principe, soit pour des fins de compatibilité avec un ordinateur donné, soit pour des fins de sauvegarde.

licence valable obtenue du détenteur des droits et viole les droits d'auteur sur le logiciel. L'employeur doit donc être prudent et s'assurer que les employés de la compagnie ne téléchargent pas ni n'utilisent des logiciels piratés sur leur ordinateur au travail[52].

1.3.3.2.2. LA RESPONSABILITÉ PAR SA PROPRE FAUTE

Certains auteurs ont soulevé la question à savoir si un employeur pouvait être tenu directement responsable en vertu de l'article 1457 C.c.Q. des dommages causés par une mauvaise utilisation d'Internet par ses employés s'il faisait défaut de surveiller et de contrôler adéquatement les actes posés par ses employés dans le cadre de l'utilisation d'Internet[53]. Sa faute serait alors la négligence.

La *Loi sur le cadre juridique des technologies de l'information*[54] prévoit depuis 2001 un régime conditionnel d'exonération de responsabilité en faveur des prestataires de services tels que les hébergeurs et les fournisseurs d'accès, visant à exonérer les intermédiaires qui ne jouent qu'un rôle passif dans la transmission de contenu sur Internet[55]. Un certain nombre de facteurs sont pris en considération dans la détermination de la responsabilité du prestataire, notamment la connaissance de l'information et le contrôle exercé sur celle-ci. Par conséquent, l'intensité de la responsabilité dépend en partie de l'intensité de contrôle que la personne exerce sur l'information diffusée[56].

En examinant ce régime, il est tentant de se demander si les employeurs pourraient

---

[52] À titre d'illustration, voir : *Krain* c. *Toronto Dominion Bank,* [2002] C.L.A.D. No. 406 (Can. Arb. Bd.). En l'espèce, l'arbitre Luborsky a confirmé le congédiement d'un employé, notamment pour avoir téléchargé et utilisé des logiciels illégalement tant pour son usage personnel que professionnel.

[53] Voir notamment Karl DELWAIDE, « L'Internet en milieu de travail et les politiques et directives relatives à l'utilisation des nouvelles technologies », Montréal, 2001, p. 6, en ligne : http://www.fasken.com/files/Publication/2bdfed9a-a187-4755-abc3-04fd5e0c6bb1/Presentation/PublicationAttachment/6bed511b-6037-4345-a9f6-09760d937b45/L_INTERNET_EN_MILIEU_DE_TRAVAIL.pdf.

[54] L.R.Q., chapitre C-1.1 (ci-après « *Loi concernant le cadre juridique des technologies de l'information* »).

[55] *Id.*, art. 22, 27, 36 et 37.

[56] Pour un exposé plus détaillé de ce régime d'exonération, voir Pierre TRUDEL, « *La responsabilité sur Internet* », Centre de recherche en droit public, Université de Montréal, 2002.

être considérés comme des fournisseurs de services Internet à l'égard de leurs employés et ainsi bénéficier du régime d'exonération de responsabilité prévu dans la loi québécoise. En effet, à première vue, les employeurs fournissent un accès à Internet à leurs employés et n'ont aucune une obligation expresse de surveiller le contenu auquel ceux-ci accèdent ou le contenu qu'ils diffusent sur Internet.

Toutefois, il apparaît que les employeurs ne peuvent être assimilés à des prestataires de services Internet et ainsi bénéficier du régime d'exonération de responsabilité qui leur est destiné. Si l'employeur pouvait bénéficier de ce régime, il serait exempté d'exercer toute surveillance active et ne pourrait alors être poursuivi pour quelque négligence. Si par ailleurs l'employeur décidait d'adopter une politique de surveillance ou d'utilisation, il aurait alors le fardeau d'effectuer un suivi et un contrôle adéquat du contenu diffusé, à défaut de quoi il pourrait être tenu responsable de tout contenu illégal.

Ce résultat irait à l'encontre du lien de subordination qui caractérise la relation employeur-employé et aurait un effet dissuasif quant au contrôle de l'utilisation d'Internet au travail, effet qui n'est certainement pas souhaitable tant pour la protection des tiers que pour celle des employés. En effet, tel que nous l'avons vu précédemment, les employeurs ont plusieurs obligations vis-à-vis de leurs employés et des tiers, que ce soit pour protéger leur dignité, leur vie privée, leurs renseignements personnels, ou encore pour assurer la sécurité des informations qu'ils détiennent sur support technologique. Il serait donc illogique que l'employeur n'ait aucune obligation de surveiller le contenu des informations qui sont reçues ou transmises par leurs employés à travers son réseau durant les heures de travail.

Bien que le régime d'exonération de responsabilité ne soit pas applicable aux employeurs, l'omission d'exercer une surveillance adéquate de l'utilisation d'Internet ne peut, à elle seule, constituer une faute directe pouvant entraîner la responsabilité de l'employeur en vertu de l'article 1457 C.c.Q. En effet, en matière de harcèlement psychologique au travail, le défaut de l'employeur de prévenir ou de faire cesser le harcèlement ne peut être considéré comme une faute directe de l'employeur. Le seul

recours de la victime de harcèlement vis-à-vis de son employeur en vertu du droit commun est celui du régime des commettants, malgré le fait que la victime puisse poursuivre l'agresseur en vertu de l'article 1457 C.c.Q.[57]. Le même raisonnement devrait donc s'appliquer pour toute utilisation fautive d'Internet au travail. La négligence ou le défaut de l'employeur d'assurer un contrôle adéquat de l'utilisation d'Internet ne devrait donc être qu'un facteur pris en considération par les tribunaux dans l'évaluation de la faute de l'employeur.

Par ailleurs, un employeur pourrait être tenu responsable en vertu de l'article 1457 C.c.Q. s'il savait ou aurait dû savoir qu'un des ses employé faisait une utilisation fautive d'Internet et omettait de prendre des mesures pour faire cesser cette utilisation fautive[58]. Prenons l'exemple d'un employé qui télécharge un logiciel piraté. Si l'employeur est au courant que la copie téléchargée est piratée et qu'il autorise tout de même son utilisation, sa reproduction ou sa distribution, il pourrait être tenu directement responsable de la violation des droits d'auteur.

1.3.3.3. Le harcèlement psychologique

Un employeur a l'obligation de fournir à ses employés un environnement de travail exempt de harcèlement ou de discrimination[59]. Depuis le 1er juin 2004, cela implique que l'employeur doit prendre des mesures raisonnables pour prévenir et pour agir (et non seulement réagir) en temps opportun afin de supprimer tout type de harcèlement accompli par ses employés dans le cadre de leur emploi[60]. À défaut de respecter une telle obligation, l'employeur peut être tenu responsable des dommages subis par la victime de harcèlement, faire l'objet d'une ordonnance de cessation, être tenu de réintégrer l'employé, de lui verser une indemnité ou encore de financer son soutien

---

[57] Julie BOURGAULT, *Le harcèlement psychologique au travail : les nouvelles dispositions de la Loi sur les normes et leur intégration dans le régime légal préexistant*, Montréal, Wilson & Lafleur, 2006, p. 104.

[58] Par analogie avec les principes énoncés dans *1267623 Ontario Inc.* v. *Nexx Online Inc.*, 46 B.L.R. (2d) 317, 45 O.R. (3d) 40, [1999] O.J. No. 2246 (Ontario Superior Court of Justice).

[59] C.c.Q., art. 2087.

[60] *Loi sur les normes du travail*, L.R.Q., chapitre N-1.1 (ci-après « L.n.t.»), art. 81.18 et 81.19.

psychologique[61].

Pour les fins du régime de responsabilité à titre de commettant pour les actes des employés dans des situations de discrimination, les tribunaux ont établi que la notion de faute commise par un employé « dans l'exécution de ses fonctions » devait être interprétée, de manière à favoriser le caractère réparateur de celle-ci. Par conséquent, en matière de discrimination, l'expression « dans l'exécution de ses fonctions » doit être interprétée comme signifiant « dans le cadre de son emploi », élargissant ainsi les situations où les employeurs peuvent être tenus responsables[62].

Les recours d'un employé victime de harcèlement psychologique sont nombreux et ne découlent pas uniquement du régime de responsabilité des commettants[63]. Une victime de harcèlement psychologique peut donc poursuivre son employeur en vertu des articles 1463 et 2087 C.c.Q, des articles 4 et 46 de la Charte québécoise, des articles 81.8, 81.19 et 123.6 de la *Loi sur les normes du travail*, et parfois de l'article 7 de la *Loi canadienne des droits de la personne*[64].

Un des exemples les plus connus en matière de harcèlement sur Internet est celui de la compagnie Chevron qui a dû payer la somme de 2,2 millions de dollars à un de ses groupes d'employés de sexe féminin en règlement d'une poursuite qui alléguait notamment le fait que Chevron avait permis l'utilisation du courrier électronique pour

---

[61] L.n.t., art. 123.15. Les recours de droit commun donnent généralement ouverture qu'à des dommages-intérêts compensatoires, et non à la réintégration dans l'emploi. Pour un exposé des réparations possibles selon les différents recours, voir J. BOURGAULT, préc., note 57, p. 117 et suiv.

[62] La Cour Suprême du Canada a énoncé les principes en matière de responsabilité de l'employeur en cas de discrimination dans les arrêts *Robichaud* c. *Canada (Conseil du trésor)*, [1987] 2 R.C.S. 84; et *Janzen* c. *Platy Enterprises Ltd.*, [1989] 1 R.C.S. 1252. Pour l'application de ces principes au Québec, voir notamment *Commission des droits de la personne et des droits de la jeunesse* c. *Centre maraîcher Eugène Guinois Jr inc.*, [2005] R.J.Q. 1315 (T.D.P.Q.); et *Commission des droits de la personne et des droits de la jeunesse* c. *Entreprise conjointe Pichette*, Lambert, Somec, J.E. 2007-1607, D.T.E. 2007T-713 (T.D.P.Q.).

[63] Pour un exposé des recours dont disposent les victimes de harcèlement sexuel, voir J. BOURGAULT, préc., note 57, p. 89 et suiv.

[64] L.R.C. 1985, c. H-6 (ci-après « *Loi canadienne des droits de la personne* »). Cette loi s'applique à toutes les industries et institution de compétence fédérales telles que la fonction publique fédérale, réglementées les compagnies d'aviation, les banques, les compagnies de téléphone, les stations télévision et de radio canadiennes.

transmettre des messages à caractère sexuel et offensant aux employés, dont un portait la mention « 25 reasons beer is better than women »[65].

Lorsqu'on parle de harcèlement psychologique, il n'est pas uniquement question de harcèlement sexuel[66]. En effet, le harcèlement psychologique se définit comme « une conduite vexatoire se manifestant soit par des comportements, des paroles, des actes ou des gestes répétés, qui sont hostiles ou non désirés, laquelle porte atteinte à la dignité ou à l'intégrité psychologique ou physique du salarié et qui entraîne, pour celui-ci, un milieu de travail néfaste »[67]. Il peut donc s'agir de tentatives d'intimidation, d'humiliation, de propos agressifs, d'attitudes visant à créer une atmosphère de travail hostile, lourde ou offensante, de menace ou de chantage, se manifestant soit de manière verbale, physique ou psychologique[68]. De plus, le harcèlement peut provenir tant de l'employeur, des collègues de travail, de tierces personnes ou encore de la clientèle de l'employeur.

Afin de fournir à ses employés un environnement de travail exempt de harcèlement ou de discrimination, l'employeur doit prendre conscience que l'accès à Internet constitue un outil supplémentaire par le biais duquel le harcèlement psychologique peut être commis par les employés. Plusieurs actes commis par le biais d'Internet peuvent en effet être couverts par la notion de harcèlement psychologique et engager la responsabilité de l'employeur, que ce soit l'envoi ou la réception de messages ou d'images à caractère sexuel sur Internet, l'utilisation d'images pornographiques

---

[65] Anne O'NEILL, « E-Mail can bounce back to hurt you », CNN.com, November 7, 2005, en ligne : http://www.cnn.com/2005/LAW/11/03/email.legal/.

[66] Le harcèlement sexuel peut être considéré comme une forme de harcèlement psychologique ou encore comme une forme de discrimination sexuelle. Pour une définition jurisprudentielle de la notion de « harcèlement sexuel », voir l'arrêt *Janzen* c. *Platy Enterprises Ltd.*, préc., note 62, 1279-1285.

[67] L.n.t., art. 81.18.

[68] À titre d'illustration, voir : *Commission des droits de la personne* c. *Habachi*, [1992] R.J.Q. 1439, D.T.E. 92T-634 (T.D.P.Q.), inf. en partie [1999] R.J.Q. 2522 (C.A.).

comme fond d'écran[69], la simple transmission de courriels intimidants à un employé[70] ou encore les menaces à l'endroit d'une collègue lors d'une session de clavardage[71].

Des employés disposant de l'accès Internet au travail pourraient par ailleurs être tentés d'aller visiter des sites Web pornographiques sans prendre de réelles précautions et sans réaliser qu'ils sont exposés au reste des employés. Si l'écran de leur ordinateur est visible pour les gens qui circulent à proximité, une telle utilisation pourrait créer un environnement hostile ou vexatoire, et constituer du harcèlement psychologique sur le lieu de travail. L'employeur doit donc agir de manière raisonnable afin de prévenir ou de faire cesser tous ces types de situation.

Bien qu'aucune décision québécoise n'ait traité expressément des obligations d'un employeur en matière de harcèlement psychologique commis par le biais d'Internet, plusieurs décisions sont venues confirmer les mesures disciplinaires prises par un employeur suite à l'envoi de messages ou de photos à connotation sexuelle par courrier électronique[72].

1.3.3.4. La protection de l'information privilégiée et confidentielle de l'entreprise

Toute entreprise a intérêt à contrôler la divulgation d'informations confidentielles la

---

[69] À titre d'illustration, voir : *Davison* v. *Nova Scotia Construction Safety Assn.*, 2005 CarswellNS 683, 55 C.H.R.R. D/327 (Nova Scotia Board of Inquiry). En l'espèce, l'affichage sur l'écran et la distribution d'une image pornographique provenant d'Internet a été considéré comme un élément de harcèlement sexuel.

[70] À titre d'illustration, voir : *Université A et Syndicat des professeures et professeurs de l'Université A (SPPUA)*, D.T.E. 2007T-601 (T.A.). En l'espèce, la plaignante a déposé un grief alléguant du harcèlement psychologique, suite à trois courriels reçus du vice-recteur. L'arbitre a toutefois conclu que la série de courriels ne constituait pas du harcèlement psychologique, compte tenu du manque de propos hostiles dans les courriels.

[71] À titre d'illustration, voir : *Syndicat des travailleuses et travailleurs de Resto-Casino de Hull (F.E.E.S.P.-C.S.N.) (section Hilton Lac Leamy) et Hilton Lac Leamy*, D.T.E. 2004T-811 (T.A.). En l'espèce, l'employeur a congédié un employé pour avoir notamment harcelé et menacé de mort une collègue au travail lors d'une session de clavardage. La plainte a été rejetée et l'arbitre a conclu que l'employeur était fondé à congédier l'employé.

[72] À titre d'illustration, voir : *C.S. Gannon* c. *Conseil du Trésor (Défense nationale)*, 2002 CRTFP 32; et *Syndicat des travailleuses et travailleurs de Resto-Casino de Hull (F.E.E.S.P.-C.S.N.) (section Hilton Lac Leamy) et Hilton Lac Leamy*, préc., note 71; et *Di Vito* v. *MacDonald Dettwiler & Associates Ltd*, [1996] B.C.W.L.D. 2036.

concernant, de même que l'utilisation qui en est faite par ses employés, contractants ou tierces parties[73]. Au Canada, la common law protège depuis longtemps l'accès et l'utilisation de ce type d'information dans le cadre d'une relation de travail[74].

La plupart des entreprises font signer des ententes de confidentialité à leurs employés ou encore incluent une clause de confidentialité dans leur contrat d'emploi, incluant une définition claire et non ambigüe de ce que l'entreprise entend par la notion d' « information confidentielle ». Cette définition inclura généralement les secrets de commerce, secrets de fabrique, le savoir-faire et les autres informations stratégiques que détient l'entreprise.

Or, en l'absence de telles ententes ou de définitions claires entendues entre les parties, il est possible de s'inspirer des facteurs énoncés par la Cour dans l'affaire australienne *Ansell Rubber Co. Pry* v. *Allied Bubber Industries Pty Ltd. (1967)*[75] afin de déterminer si une information possède un caractère confidentiel et quel est son degré de confidentialité.

Les secrets de commerce d'une compagnie, qui peuvent inclure son savoir-faire, se définissent comme étant l'information qui n'est généralement pas connue dans l'industrie ou facilement accessible, qui a une valeur commerciale et pour laquelle son propriétaire prend des mesures raisonnables pour la garder secrète[76].

Les secrets de commerce d'une entreprise ou tout autre type d'information confidentielle lui appartenant, font non seulement partie intégrante de son actif, mais peuvent constituer un atout très précieux sur le marché. Les listes de clients, les listes

---

[73] Au Canada, contrairement aux brevets et aux droits d'auteur, la protection juridique accordée à l'information confidentielle provient de la common law.

[74] P. Bradley LIMPERT, *Technology Contracting : Law, Precedents and Commentary*, Toronto, Carswell, 2009, feuilles mobiles, à jour en 2009 (release 2009-1), p. I-16.1 à I-22.1.

[75] [1967] V.Q. 37, [1972] R.P.C. 811 (Australia Vic. Sup. Ct.). Ces facteurs ont été cités dans l'affaire *Pharand Ski Corp. v. Alberta*, (1991) 37 C.P.R. (3d) 288 (ABQB). Voir également P. Bradley LIMPERT, préc., note 74, p. I-5.

[76] Laurent CARRIÈRE, « Les secrets de commerce : notions générales », 1996, *robic.ca*. Pour une définition jurisprudentielle canadienne, voir *Pharand Ski Corp. v. Alberta*, préc., note 75, p. 316.

de prix, les plans de marketing, les plans d'affaires, les techniques de fabrication, les résultats de recherche, les structures financières et commerciales et tout autre type d'information commerciale, sont autant d'exemples d'information confidentielle qui peuvent être mis en péril par l'utilisation d'Internet des employés[77].

Une divulgation non autorisée de ces informations peut avoir des conséquences néfastes pour l'entreprise, notamment la perte de protection juridique liée aux secrets de commerce, ou encore la perte de brevetabilité d'une invention[78].

À titre d'exemple, dans l'affaire *Hartco, l.p.* c. *Neulogic Sales Inc.*[79] un employé déloyal a communiqué par courrier électronique avec les concurrents de l'entreprise et a mis en danger ses secrets de commerce[80].

Une étude sur les habitudes des utilisateurs de courrier électronique en entreprise

---

[77] Les critères applicables pour bénéficier de la protection juridique accordée à l'information confidentielle sont énoncés dans l'arrêt *Lac Minerals Ltd.* C. *International Corona Resources Ltd.*, (1989) 2 R.C.S. 574, 635-636, dans lequel le juge Laforest cite, au nom de la majorité, les propos du juge Megarry dans l'arrêt *Coco* v. *A.N. Clark (Engineers) Ltd.*, [1969] R.P.C. 41 (Chancery Division, England and Wales), p. 47 : [TRADUCTION] « Tout d'abord les renseignements eux-mêmes, selon les termes de lord Greene, M.R., à la p. 215 de l'arrêt Saltman, doivent « posséder le caractère confidentiel nécessaire ». Deuxièmement, leur communication doit avoir eu lieu dans des circonstances ayant donné naissance à une obligation fondée sur des rapports de confiance. Troisièmement, il doit y avoir un emploi non autorisé des renseignements au détriment de la partie qui les a communiqués. »

[78] Une invention ne peut plus faire l'objet d'une demande de brevet si elle a été divulguée au public plus d'un an suivant le dépôt de la demande (*Loi sur les brevets,* L.R., 1985, ch. P-4, art. 28.2).

[79] B.E. 2006BE-177 (C.S.). En l'espèce, la Cour supérieure a accueilli une requête de type Anton Piller sur la base d'allégations suivant lesquelles le défendeur, un employé de la demanderesse, avait transmis des informations confidentielles par courrier électronique à des tiers, possiblement des compétiteurs de la demanderesse.

[80] Voir également la décision *Brunswick News Inc.* v. *Langdon,* 2007 NBQB 424, 858 A.P.R. 325, 334 N.B.R. (2d) 325. En l'espèce, l'éditeur d'un journal local, qui envisageait de créer un journal faisant compétition à son employeur, avait transmis plusieurs informations confidentielles par voie de courrier électronique sur son compte de courrier personnel à partir de son lieu de travail. Le défendeur Langdon avait notamment transmis la liste de clients, le plan d'affaires, le budget et les documents relatifs aux stratégies de ventes pour l'année à venir. Aux États-Unis, voir *Borland Int'l, Inc.* v. *Eubanks*, Cal. Sup. Ct., Civ. Case No. 123059 (Santa Cruz 1992). En l'espèce, le vice-président de Borland International, qui envisageait d'aller travailler pour un compétiteur, a envoyé sans autorisation de l'information confidentielle appartenant à l'employeur, notamment des données sur les clients et des données techniques, à un compétiteur. Immédiatement après avoir transmis ces informations par courriel, le vice-président a démissionné de son poste et est allé travailler chez le compétiteur en question. Voir également *People* v. *Eubanks*, 927 P.2d 310 (Cal. 1996).

publiée en 2005[81] révèle que 6 % des utilisateurs professionnels avouent avoir divulgué des données d'entreprise confidentielles par e-mail auprès de personnes non habilitées. De plus, selon une étude américaine[82], 12% des messages instantanés contiendraient des informations confidentielles ou privilégiées.

Par ailleurs, la confidentialité des informations ne concerne pas uniquement l'entreprise elle-même. Elle peut également toucher des personnes physiques qui font affaire avec celle-ci, tels que des employés ou des clients. À cet égard, plusieurs lois provinciales[83] et fédérales[84] imposent des obligations aux personnes qui recueillent, détiennent, utilisent et communiquent des renseignements personnels[85], ou encore aux entreprises qui transmettent et conservent des renseignements confidentiels sur support électronique[86]. Les entreprises et organismes québécois doivent donc prendre des mesures pour assurer la protection de ces renseignements et éviter que ceux-ci soient divulgués à des personnes non autorisées, à défaut de quoi elles peuvent être condamnées à payer des amendes pénales de même que des dommages-intérêts[87].

---

[81] RADICATI GROUP, INC. AND MIRAPOINT, INC., *Corporate Email User Habits*, California, September 2005, en ligne : http://www.imerja.com/files/file/Reports/Radicati%20Group/Email%20user%20habits.pdf.

[82] AMERICAN MANAGEMENT ASSOCIATION (AMA) AND THE EPOLICY INSTITUTE, *2006 Workplace W-Mail, Instant Messaging & Blog Survey*, préc., note 14.

[83] Au Québec, voir C.c.Q., art. 37-41; *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1 (ci-après « Loi sur l'accès »); et *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1 (ci-après « Loi sur le secteur privé »).

[84] Au fédéral, voir *Loi sur la protection des renseignements personnels*, L.R., 1985, ch. P-21 (ci-après « L.p.r.p. »); et *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5 (ci-après « L.p.r.p.d.é. »).

[85] L'article 2 de la Loi sur le secteur privé définit la notion de « renseignement personnel » comme étant « tout renseignement qui concerne une personne physique et permet de l'identifier ». La Loi sur l'accès contient une disposition similaire (art. 54), de même que les lois fédérales (L.p.r.p.d.é., art. 2 ; et L.p.r.p., art. 3).

[86] *Loi concernant le cadre juridique des technologies de l'information*, art. 25 et 34. Pour un énoncé général des obligations qui découlent de la *Loi sur le cadre juridique des technologies de l'information*, voir Vincent GAUTRAIS, « Afin d'y voir clair, Guide relatif à la gestion des documents technologiques », Fondation du Barreau du Québec, Montréal, novembre 2005, en ligne : http://www.fondationdubarreau.qc.ca/pdf/publication/Guidetech_FR.pdf.

[87] Loi sur l'accès, art. 158 à 165; Loi sur le secteur privé, art. 91-93; et L.p.r.p.d.é., art. 16. Pour des illustrations de ce genre de situation dans le cadre d'un grief pour congédiement, voir : *Laboratoire de santé publique et Syndicat canadien de la fonction publique, section locale 2667*, [1992] T.A. 23, D.T.E. 92T-34; et *Syndicat des fonctionnaires municipaux de Québec et Ville de Québec,* [1995] T.A. 997, D.T.E. 95T-1337.

Bien que les employés soient soumis à une obligation de loyauté et de confidentialité vis-à-vis leur employeur[88], ils peuvent facilement avoir accès à de l'information confidentielle et la transmettre par courrier électronique à des tiers, ou encore la diffuser sur Internet, que ce soit intentionnellement ou par inadvertance. Dans ce contexte, la mise en place d'une surveillance de l'utilisation d'Internet constitue un des outils à la disposition des employeurs permettant d'éviter ces risques.

1.3.3.5. La protection de la vie privée, de l'image et de la réputation de l'entreprise

La vie privée d'une entreprise de même que son image et sa réputation peuvent également être mises en danger par une mauvaise utilisation d'Internet par les employés.

À titre d'exemple, un employé s'est déjà fait prendre à avoir publié, sur un forum de discussion, un texte offensant à caractère diffamatoire, qui portait sa signature accompagnée du nom de l'employeur[89]. La Cour a conclu que les actes de l'employé avaient porté atteinte à la vie privée de l'entreprise et que le défendeur avait enfreint son devoir de loyauté vis-à-vis de son employeur, soulignant que ce devoir avait préséance sur la liberté d'expression de l'employé[90].

Que ce soit en transmettant des messages offensants par le biais du courrier électronique de l'entreprise, en signant un billet sur un blog ou un message sur un forum de discussion avec l'adresse de courrier électronique de l'entreprise, ou simplement en communiquant des informations diffamatoires ou erronées sur leur employeur par courrier électronique ou sur le Web, les employés déloyaux disposent, grâce à Internet, de nombreux outils pour nuire à l'image et à la réputation de leur

---

88 C.c.Q., art. 2088.

89 *Arpin* c. *Grenier*, préc., note 36.

90 Voir également *D'Astous* c. *Sesno,* [2001] R.J.D.T. 85, D.T.E. 2001T-25 (C.Q.). En l'espèce, l'employé avait créé un site Internet pour l'entreprise avec un lien direct sur son site personnel, et avait, parallèlement, créé un autre site Internet en reproduisant textuellement le site de l'employeur. La Cour a conclu que le comportement de l'employé avait nuit à la crédibilité de l'entreprise et avait créé de la confusion. Elle a condamné l'employé à des dommages pécuniaires (3,000.00$).

employeur. Bien que les tribunaux accordent normalement des dommages-intérêts en réparation du préjudice causé à l'entreprise, les affaires *Arpin*[91] et *D'Astous*[92] démontrent que les montants accordés sont plutôt minces. Par conséquent, les entreprises préféreront éviter ce genre de situations en contrôlant du mieux qu'elles peuvent l'utilisation d'Internet par les employés.

1.3.3.6. La baisse de productivité des employés

Bien que l'implantation de l'accès à Internet dans les entreprises vise principalement à accroître la productivité des employés, il n'en demeure pas moins que les entreprises qui ne contrôlent pas suffisamment son utilisation risquent d'avoir certaines surprises quant à l'utilisation qui en est faite par certains employés.

En effet, il serait illusoire de croire qu'Internet est utilisé par les employés uniquement à des fins professionnelles. Au même titre que le téléphone, Internet est un outil de communication qui, bien que fourni par l'employeur pour des fins professionnelles, permet facilement de communiquer avec ses proches, son réseau social ou autre, ou encore d'effectuer certaines tâches de type personnel, telles que consulter la météo, lire les nouvelles, faire du magasinage en ligne ou chercher une destination voyage.

À cet effet, les statistiques démontrent qu'une grande proportion des employés, soit environ deux québécois sur cinq, utilise Internet à des fins personnelles[93].

À première vue, le fait qu'Internet soit utilisé à des fins personnelles n'est pas si surprenant. En effet, le téléphone est également un outil de communication qui peut

---

[91] Préc., note 36.

[92] Préc., note 90.

[93] CROP, « Visite d'Internet au Travail », dans *CROP-Express*, #35, Québec, Février 2007, en ligne : http://www.orhri.org/presse/2007/070402_CROP_internet-trav.pdf, p. 8. Au niveau de la population canadienne, un sondage réalisé en 2006 révèle que 43% de la population active canadienne, utilise Internet à des fins personnelles à partir du travail : IPSOS REID, *The 2006 Canadian Inter@ctive Reid Report*, Canada, 2006. Aux États-Unis, selon HARRIS INTERACTIVE, préc., note 4, p. 3, 61% des employés d'entreprises de plus de 100 employés utilisent Internet à des fins personnelles.

être utilisé par les employés pour des fins personnelles et, à ce que nous sachions, son utilisation n'a pas été bannie des entreprises à tout le moins au niveau local. La question est plutôt de savoir dans quelle proportion les employés qui disposent de l'accès à Internet au travail l'utilisent-ils à des fins personnelles plutôt que pour travailler. Selon le sondage CROP, les employés québécois consacreraient en moyenne 22 minutes par jour à utiliser Internet à des fins personnelles[94].

Évidemment, il ne s'agit que d'une moyenne et il peut parfois arriver que les employés la dépassent de beaucoup. Un exemple flagrant d'un tel abus est l'affaire *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* et *C.A.E. Électronique Ltée*[95], dans laquelle un employé s'est fait prendre à avoir passé plus de 329 heures de travail réparties sur quatre mois et demi à naviguer sur des sites Internet, incluant des sites pornographiques[96].

Plusieurs exemples[97] illustrent des manquements graves au devoir de fournir une prestation de travail adéquate dans des temps raisonnables[98], de même qu'au devoir de loyauté des employés[99]. Afin d'éviter ces violations et éviter une baisse de

---

[94] CROP, préc., note 93, p. 9. Selon cette étude, 62% des québécois consacrent en moyenne 15 minutes ou moins par jour à naviguer sur Internet à des fins autres que professionnelles, et 35% y consacrent plus de 15 minutes. Selon HARRIS INTERACTIVE, préc., note 4, p. 3, les employés américains passeraient en moyenne 3,1 heures par semaine à naviguer sur des sites Internet à des fins personnelles.

[95] [2000] R.J.D.T. 327, D.T.E. 2000T-157 (T.A.).

[96] Voir également l'affaire *Syndicat des spécialistes et professionnels d'Hydro-Québec, section locale 4250 (SCFP-FTQ) et Hydro-Québec*, [2007] R.J.D.T. 1172, D.T.E. 2007T-541 (T.A.), dans laquelle l'employé avait passé en moyenne une heure et quarante minutes par jour à utiliser Internet à des fins personnelles pendant les heures de travail et ce, durant une période de neuf mois.

[97] Pour des exemples jurisprudentiels de vol de temps dans le contexte de l'utilisation d'Internet au travail, voir : *Fairmont Le Reine Élizabeth et Syndicat des travailleuses et travailleurs de l'Hôtel Le Reine Élizabeth (C.S.N.)*, D.T.E. 2004T-1168 (T.A.); *Syndicat des employés de bureau de Thetford Mines et Thetford Mines (Ville de)*, D.T.E. 2005T-254 (T.A.); *Syndicat canadien de la fonction publique, section locale 4140 et Centres jeunesse de l'Outaouais*, D.T.E. 2005T-961, AZ-50338981 (T.A.); *Montour Ltée et Syndicat des employés et employés de la Cie Montour (CSN)*, D.T.E. 2007T-195 (T.A.); *Syndicat des employés municipaux de Beloeil (SCFP) et Beloeil (Ville de)*, D.T.E. 2007T-874 (T.A.); *Collège Ahuntsic* c. *Syndicat du personnel de soutien du Collège Ahuntsic*, D.T.E. 2007T-889 (T.A.); et *Syndicat de la fonction publique du Québec – Fonctionnaires et Québec (Ministère de l'Emploi et de la Solidarité sociale)*, D.T.E. 2008T-642 (T.A.).

[98] Devoir qui découle des articles 2085 C.c.Q. Voir à cet égard K. DELWAIDE, préc., note 53, p. 4.

[99] C.c.Q., art. 2088. L'obligation d'honnêteté et de loyauté emporte celle de travailler toutes les heures rémunérées. Voir à cet effet *Furfaro et Costco Canada inc.*, D.T.E. 2000T-920 (C.T.).

productivité, les employeurs ont intérêt à contrôler les activités menées par leurs employés par le biais de l'accès à Internet au travail.

1.4. La surveillance

1.4.1. Les outils et moyens pratiques à la disposition des employeurs

Tel qu'exposé précédemment, bien que l'utilisation d'Internet au travail puisse être très avantageuse pour un employeur, les risques que ce dernier court en fournissant un accès Internet à ses employés demeurent présents et nombreux. Heureusement, les employeurs ont à leur disposition plusieurs moyens leur permettant de prévenir, de détecter et d'éliminer ces risques de façon à pouvoir maximiser les avantages liés à l'utilisation d'Internet au travail.

Exercer une surveillance des employés au niveau de l'utilisation d'Internet constitue l'un des ces moyens. Cette pratique est d'ailleurs de plus en plus répandue dans les entreprises, tel qu'illustré dans une étude effectuée conjointement par l'American Management Association (AMA) et The ePolicy Institute en 2007[100]. Les résultats de cette étude qui nous intéressent plus particulièrement sont les suivants : (i) 43% des employeurs américains surveillent la boîte de courrier électronique de leurs employés; (ii) 66% surveillent les connections au réseau Internet de leurs employés. De ce nombre, 39% le font de manière continue, 24% régulièrement et 23% occasionnellement; (iii) 45% des employeurs américains surveillent le contenu, les frappes et le temps consacré sur son clavier d'ordinateur au travail,; (iv) 43% des employeurs américains surveillent le contenu des fichiers enregistrés sur l'ordinateur de l'employé; (v)12% surveillent la blogosphère pour connaître ce que les employés disent au sujet de l'employeur; et (vi) 10% surveillent les sites de réseau social (ex. Facebook, MySpace, etc.).

Outre la surveillance, les employeurs peuvent décider de : (i) implanter des

---

[100] AMERICAN MANAGEMENT ASSOCIATION (AMA) AND THE EPOLICY INSTITUTE, *2007 Electronic Monitoring & Surveillance Survey*, États-Unis, 2007, en ligne : http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf.

techniques de filtrage du contenu dans les communications Internet ou la navigation sur le web[101]; (ii) bloquer le téléchargement de fichiers ; (iii) imposer des sanctions disciplinaires aux employés qui font une mauvaise utilisation d'Internet au travail[102] ; ou encore (iv) imposer des règles quant à l'utilisation d'Internet au travail à l'aide de politiques ou de directives[103]. Bien que ces outils et moyens de contrôle ne fassent pas l'objet du présent mémoire, il est néanmoins important de savoir que l'employeur peut avoir intérêt à utiliser ces diverses méthodes parallèlement à la surveillance, de façon à maximiser la diminution des risques liés à l'utilisation d'Internet au travail.

Un employeur qui décide de surveiller l'utilisation d'Internet par ses employés dispose par ailleurs de plusieurs options, que ce soit au niveau de l'étendue de la surveillance, du type de surveillance et de l'intensité de la surveillance exercée. Dépendamment des besoins de l'employeur, certains types de surveillance seront plus appropriés que d'autres. Voyons maintenant les différents types de surveillance offerts aux employeurs.

1.4.2. Les types de surveillance

1.4.2.1. Généralités

Avec la popularité grandissante de la surveillance de l'utilisation d'Internet au travail, de plus en plus de produits et services sont offerts aux employeurs. Pour les fins de la présente recherche, nous nous limiterons à exposer les technologies qui leur permettent de surveiller l'utilisation d'Internet au travail, que ce soit au niveau du courrier électronique, de la messagerie instantanée, du téléchargement de fichiers en ligne, de la publication de contenu sur le web (notamment dans des forums de discussion, dans des blogs ou autres sites) ou de la navigation sur le Web.

---

[101] *Id.*, p. 5 et 6 (statistiques sur l'implantation de techniques de filtrage de contenu au travail).

[102] *Id.*, p. 8 et 9 (statistiques sur le nombre d'employés ayant imposé des mesures disciplinaires pour une mauvaise utilisation d'Internet ou du courrier électronique).

[103] Pour des statistiques sur l'adoption d'une politique d'utilisation d'Internet ou du courrier électronique au travail, voir CEFRIO, *NET Québec 2008,* préc., note 2, p. 4; et AMERICAN MANAGEMENT ASSOCIATION (AMA) AND THE EPOLICY INSTITUTE, *2007 Electronic Monitoring & Surveillance Survey*, préc., note 100.

Nous tenons quand même à souligner brièvement l'existence des technologies de surveillance au niveau des autres outils informatiques utilisés par les employés. Certains logiciels vont par exemple indiquer le nombre de touches du clavier d'ordinateur tapées par minute, le temps et la localisation précise de chacune des erreurs commises par l'utilisateur, le temps passé à compléter chacune des tâches à l'aide de l'ordinateur, de même que les temps de pause. D'autres logiciels vont surveiller le temps consacré par les utilisateurs dans la rédaction de documents, le nombre de brouillons d'un document et le nombre de révisions par ligne. Les employeurs peuvent par ailleurs faire appel à des enquêteurs technologiques (*Computer Forensics)* pour extraire ou reconstruire des communications électroniques transmises, reçues et enregistrées sur le disque dur d'un ordinateur, et ce même après que celles-ci aient fait l'objet de tentative de suppression par l'utilisateur. Bien que ces types de surveillance ne soient pas couverts spécifiquement par notre analyse, compte tenu qu'il s'agit de l'utilisation des équipements informatiques plutôt que de l'accès Internet, ils peuvent néanmoins être utilisés parallèlement par l'employeur en complément des outils de surveillance de l'utilisation d'Internet.

Il convient par ailleurs de rappeler que certains employeurs surveillent l'utilisation d'Internet de leurs employés sans nécessairement avoir recours à des logiciels informatiques conçus à cette fin. Ils peuvent en effet simplement observer ou espionner de loin l'écran d'ordinateur d'un employé. D'ailleurs, les données de l'AMA et The ePolicy Institute de 2007 révèlent que 40 % des employeurs qui surveillent le courrier électronique dédient directement une personne à la lecture et l'analyse manuelle des courriers électroniques de leurs employés[104]. Bien que la surveillance physique ne soit pas aussi efficace et complète que la surveillance électronique, il n'en demeure pas moins qu'elle constitue un moyen de surveillance de l'utilisation d'Internet et, par conséquent, est soumise aux principes énoncés dans

---

[104] AMERICAN MANAGEMENT ASSOCIATION (AMA) AND THE EPOLICY INSTITUTE, *2007 Electronic Monitoring & Surveillance Survey*, préc., note 100, p. 5.

le présent mémoire.

1.4.2.2. Les techniques de surveillance de l'utilisation d'Internet au travail

La surveillance de l'utilisation d'Internet peut s'exercer de différentes façons. Elle peut être individuelle, c'est-à-dire limitée à un seul employé, ou encore généralisée à l'ensemble des employés d'une compagnie. Elle peut être ponctuelle, c'est-à-dire limitée à une situation bien précise, ou encore permanente, c'est-à-dire exercée de manière continue dans le temps. Un employeur exercera souvent une surveillance ponctuelle suite à un incident ayant fait naître des doutes quant à l'utilisation d'Internet par un employé. L'employeur décidera alors de mener une enquête plus poussée afin de connaître l'étendue et la gravité de l'utilisation fautive d'Internet par l'employé en question. Finalement, la surveillance pourra être effectuée par le biais d'un visionnement simultané, c'est-à-dire que les activités des employeurs seront surveillées au fur et à mesure qu'elles sont effectuées, ou encore consister en un enregistrement pour fins de consultation ultérieure.

Les logiciels de surveillance peuvent soit être installés au niveau du serveur du fournisseur d'accès Internet de l'employeur, ou encore directement dans le poste de travail de l'employé[105]. La surveillance basée au niveau du serveur sera particulièrement utile si l'employeur souhaite exercer une surveillance générale et étendue à l'ensemble ou à un groupe d'employés.

Les logiciels de surveillance actuellement disponibles sur le marché remplissent généralement plusieurs fonctions[106]. La plupart fourniront des rapports détaillés

---

[105] Certains logiciels vont offrir les deux possibilités. Voir notamment le logiciel *Track4Win*.

[106] Voir notamment le logiciel *CyberSpy* qui enregistre les conversations par messagerie instantanée, les touches du clavier utilisées, les sites web visités, capture l'écran d'ordinateur, enregistre les documents ouverts, les mots de passe utilisés et les courriels écrits. Voir également les logiciels suivants : *Golden Eye, AceSpy, XPCSpy Pro, Personal Inspector, PC Acme Pro, Spectorsoft, Mariansoft PC Police Professional, Invisible Keylogger, KeyDevil* et *Employee Activity LIVE Watcher Server*. Pour un tableau comparatif de différents logiciels de surveillance de l'utilisation d'Internet offerts actuellement sur le marché, voir H. Joseph WEN et al., « Internet Usage Monitoring in the Workplace : Its Legal Challenges and Implementation Strategies », *Information Systems Management,* (2007) 24 (n° 2), en ligne :

indiquant l'historique des activités de l'employé sur Internet, que ce soit sur le Web ou au niveau du courrier électronique[107]. Quant aux informations pouvant être fournies et des activités pouvant être surveillées, les possibilités sont variées. Les employeurs peuvent surveiller tant l'utilisation de la messagerie instantanée, du courrier électronique, des connexions Internet, des activités sur le Web, surveiller les logiciels utilisés, des jeux téléchargés, des fichiers contenus sur le disque dur, connaître le volume de bites consommé dans l'utilisation de l'accès Internet et le temps consacré aux différentes activités Internet.

En ce qui a trait à la navigation sur le Web, certains logiciels vont capturer l'image se trouvant sur l'écran d'ordinateur de l'employé à des intervalles réguliers pour ensuite les compresser pour analyser le travail effectué sur l'ordinateur de l'employé. D'autres vont révéler toutes les activités effectuées incluant les sites web visités, le temps passé sur chaque site, et la nature des sites visités[108].

Au niveau du courrier électronique, il est possible d'enregistrer automatiquement tous les messages ayant transité sur le serveur central de la compagnie, de façon à ce que ces données soient conservées pour fins de consultation ultérieure. Certains logiciels vont indiquer la fréquence des messages entrant ou sortant de la boîte de courrier électronique de l'employé, allant même jusqu'à recouvrer et analyser les messages brouillons rédigés et supprimé avant l'envoi[109]. D'autres vont fournir tant le nom du destinateur, le nom du destinataire, le nombre de mots contenus dans le message, le temps passé par l'employé à lire ou à écrire le message, le nombre de fichiers joints,

---

http://road.uww.edu/road/peltierj/Privacy/Internet%20usage%20monitoring%20in%20the%20workplace.pdf, p. 185.

[107] Michael GEIST, « Computer and E-mail Workplace Surveillance in Canada: The Shift from reasonable expectation of privacy to reasonable surveillance », rapport préparé pour le Conseil Canadien de la Magistrature, Mars 2002, en ligne: http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_Surveillance_2002_en.pdf, p. 10.

[108] Gail LASPROGATA, « Regulation of Electronic Employee Monitoring : Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada », 2004 *Stan. Tech. L. Rev.* 4, en ligne : http://stlr.stanford.edu/pdf/Lasprogata-RegulationElectronic.pdf, par. 20.

[109] M. GEIST, préc., note 107, p. 10.

ou encore la nature personnelle ou professionnelle du message.

Quant à la surveillance du téléchargement et du partage de fichiers sur Internet, des logiciels permettent de surveiller les disques durs des ordinateurs de façon à identifier les fichiers de nature pornographique qui s'y trouvent et les fichiers audio ou vidéo qui ont été téléchargés en violation des droits d'auteurs ou des politiques de l'entreprise[110].

À la lumière de ce qui précède, nous pouvons affirmer que les logiciels de surveillance offerts sur le marché permettent aux employeurs de soutirer facilement toute une gamme d'informations au niveau de l'utilisation d'Internet par les employés. De plus, la surveillance de l'utilisation d'Internet diffère des autres types de surveillance électronique du fait qu'elle permet aux employeurs de surveiller simultanément tous ses employés et d'obtenir beaucoup plus d'information. Alors qu'avec la surveillance traditionnelle les employés savaient quand est-ce que le patron les surveillait, avec la surveillance de l'utilisation d'Internet le patron peut être là en tout temps. Il est donc très tentant pour un employeur d'avoir recours à ces outils.

Par ailleurs, bien que l'exercice de la surveillance puisse être légitime lorsque l'on considère tous les risques liés à l'utilisation d'Internet au travail, encore faut-il se demander si l'employeur a le droit d'exercer ce type de surveillance et jusqu'où va ce droit. Il ne faut pas oublier que les employés, de même que les tiers, jouissent de certains droits qui peuvent venir limiter les droits de l'employeur dans l'exercice de cette surveillance.

Nous exposerons maintenant les intérêts concurrents en matière de surveillance de l'utilisation d'Internet au travail, à savoir les fondements du droit de surveillance de l'employeur et les limites auxquelles se heurte l'employeur dans l'exercice de ce

---

[110] G. LASPROGATA, préc., note 108, par. 20.

droit. Cette analyse est essentielle afin de déterminer la manière dont la surveillance peut être légalement exercée.

2. LES ENJEUX LIÉS À LA SURVEILLANCE DE L'UTILISATION D'INTERNET AU TRAVAIL

2.1. Les fondements du droit de surveillance de l'employeur

En principe, un employeur a le droit de surveiller l'utilisation d'Internet par ses employés au travail. Ce droit se fonde sur le pouvoir de direction et de contrôle de l'employeur[111], lequel découle du lien de subordination qui le lie à ses employés. Ce principe est toutefois sujet à certaines réserves qui feront l'objet de la prochaine sous-section. Pour l'instant, voyons les fondements qui sont à la base du droit de surveillance de l'employeur, afin d'être en mesure d'en délimiter l'étendue.

2.1.1. Le pouvoir de direction et de contrôle

2.1.1.1. Généralités

En concluant un contrat de travail, un employé consent en quelque sorte à se placer en situation d'inégalité vis-à-vis de son employeur. Cette situation d'inégalité est due au lien de subordination qui lie l'employé à l'employeur et donne à l'employeur la faculté « de déterminer le travail à exécuter, d'encadrer cette exécution et de la contrôler »[112]. Même si dans certains cas l'employé dispose d'une grande liberté d'exécution pratique, il demeure néanmoins assujetti à un lien de subordination avec son employeur.

L'existence d'un lien de subordination entre l'employé et l'employeur constitue l'une

---

[111] K. DELWAIDE, préc., note 53, p. 20; et Rhéaume PERREAULT, « L'adoption d'une politique d'utilisation du courriel et d'Internet : où est le bogue? », dans S.F.P.B.Q., vol. 134, *Développements récents en droit du travail (2000),* Cowansville, Éditions Yvon Blais, p. 71, à la page 93.

[112] Robert P. GAGNON, *Le Droit Du Travail Du Québec*, 8e éd., Cowansville, Éditions Yvon Blais, 2008, n° 92, p. 69. À titre d'illustration, voir : *Brown* c. *Industrielle Alliance valeurs mobilières inc.*, 2007 QCCS 1602, AZ-50427179, par. 161-162.

des caractéristiques fondamentales du contrat de travail[113], lequel se définit de la façon suivante à l'article 2085 C.c.Q. :

> « Le contrat de travail est celui par lequel une personne, le salarié, s'oblige, pour un temps limité et moyennant rémunération, à effectuer un travail sous la direction ou le contrôle d'une autre personne, l'employeur. »[114]

C'est d'ailleurs ce qui distingue le contrat de travail du contrat de services ou d'entreprises, pour lequel aucun lien de subordination n'existe et pour lequel le prestataire de services ou l'entrepreneur a le libre choix des moyens d'exécution du contrat[115].

Le lien de subordination qui caractérise le contrat de travail justifiera notamment les obligations du salarié envers son employeur, telles que la prestation, la disponibilité, la discrétion, la loyauté et la convivialité, et il expliquera le statut d'autorité de l'employeur et les pouvoirs qui s'y rattachent, notamment le pouvoir de direction et de contrôle qui en découle[116].

Le pouvoir de direction et de contrôle de l'employeur permet à l'employeur de contrôler la gestion, l'organisation et tous les aspects économiques de l'entreprise, de façon à s'assurer de son bon fonctionnement[117]. Compte tenu que l'activité du salarié

---

[113] *Cabiakman* c. *Industrielle-Alliance Cie d'Assurance sur la Vie,* [2004] 3 R.C.S. 195, 206; *Bureau d'études Archer inc.* c. *Dessureault*, 2006 QCCA 1556, AZ-50399426, par. 27; *Centre hospitalier régional de Trois-Rivières (Pavillon St-Joseph) et Syndicat professionnel des infirmières et infirmiers de Trois-Rivières (Syndicat des infirmières et infirmiers Mauricie—Coeur-du-Québec)*, [2006] R.J.D.T. 397, D.T.E. 2006T-209, (T.A.), par. 246 et suiv.; Marie-France BICH, « Le contrat de travail : Code civil du Québec, Livre cinquième, titre deuxième, chapitre septième (articles 2085-2097 C.c.Q.) », dans Barreau du Québec et Chambre des notaires du Québec (dir.), *La réforme du Code civil : obligations, contrats nommés*, t. 2, Sainte-Foy, P.U.L., 1993, p. 741, à la page 752.

[114] C.c.Q., art. 2085 (nos soulignés).

[115] C.c.Q., art. 2099.

[116] Fernand MORIN et Jean-Yves BRIÈRE, *Le droit de l'emploi au Québec*, 3e éd., Montréal, Wilson et Lafleur, 2006, p. 234.

[117] *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*, [1999] R.J.Q. 2229, [1999] R.J.D.T. 1075 (C.A.), 1088 : « La relation de travail implique (...) la reconnaissance d'un pouvoir de direction et de contrôle, justifié fonctionnellement par la nécessité d'aménager et de diriger le travail afin d'assurer la réalisation des finalités de l'entreprise. » Voir également K. DELWAIDE, préc., note 53, p. 3; et R. PERREAULT, préc., note 111, à la page 75.

s'intègre au cadre tracé par l'employeur et s'effectue au bénéfice de celui-ci, il est normal que l'employeur dispose d'un pouvoir de direction et de contrôle à son égard[118].

Tel qu'il ressort des propos du tribunal d'arbitrage dans la décision *Centre hospitalier régional de Trois-Rivières (Pavillon St-Joseph) et Syndicat professionnel des infirmières et infirmiers de Trois-Rivières (Syndicat des infirmières et infirmiers Mauricie—Coeur-du-Québec)*[119], le pouvoir de direction et de contrôle constitue un pouvoir de nature discrétionnaire qui doit être exercé de manière raisonnable :

> « C'est ainsi que dans la direction et le contrôle de son personnel, l'employeur possède une discrétion étendue lorsqu'il s'agit d'établir et de faire respecter les procédures de travail, les règles et les usages du milieu de travail, d'évaluer le rendement des salariés et de contrôler la qualité du travail qu'ils accomplissent : tout cela fait partie de l'exercice normal du droit de direction et il est entendu qu'il peut en résulter du stress et des désagréments. Tout cela fait partie de la normalité des choses. Ce n'est donc qu'en cas d'exercice déraisonnable du droit de direction que l'on peut parler d'abus de droit. »[120]

À cet égard, il est important de souligner que les pouvoirs de l'employeur ne peuvent être exercés qu'en relation avec les obligations que doivent remplir les employés[121]. En d'autres mots, toute directive, surveillance ou autre type de manifestation du pouvoir de contrôle et de direction de l'employeur doit avoir un rapport direct avec la prestation des obligations des employés[122].

Par ailleurs, le pouvoir de direction et de contrôle prendra diverses formes en fonction de la nature du travail et du degré d'autonomie et de spécialisation de l'employé. Par

---

[118] M.-F. BICH, préc., note 113, à la page 752.

[119] Préc., note 113.

[120] *Id.*, par. 250.

[121] Claude D'AOUST, « L'électronique et la psychologie dans l'emploi », dans D. NADEAU & B. PELLETIER (dir.), *Relation d'emploi et droits de la personne : évolution et tensions!*, Cowansville, Éditions Yvon Blais, 1994, p. 35, à la page 37.

[122] F. MORIN et J.-Y. BRIÈRE, préc., note 116, p. 235 : « Cette autorité et cette désobéissance s'entendent aux seules fins de la prestation de travail, soit la durée où le salarié est en disponibilité professionnelle, pour le compte de l'entreprise. »

exemple, le contrôle exercé à l'égard d'un employé spécialisé ou dont l'exercice requiert une grande latitude professionnelle portera généralement sur la vérification de la régularité et de la qualité du travail de l'employé plutôt que sur sa façon de l'exécuter. Dans ce contexte, le contrôle sera moins sévère ou effectué différemment comparativement à un représentant des ventes ou autre métier peu spécialisé[123].

Dans tous les cas et peu importe son degré d'intensité, l'exercice d'une surveillance de l'utilisation d'Internet au travail constitue l'une des facettes de ce pouvoir de direction et de contrôle au profit de l'employeur. Tel que mentionné, ce pouvoir doit toutefois être exercé de manière raisonnable et dans les limites de l'objet du contrat de travail. Afin d'être exercé légitimement, le pouvoir de direction et de contrôle devra viser le bon fonctionnement de l'entreprise, lequel objectif pourra viser plus particulièrement à éliminer les risques liés à l'utilisation d'Internet, à s'assurer que les employés respectent leurs obligations, ou encore que les employés jouissent d'un environnement de travail dénué de toute discrimination.

2.1.1.2. L'objectif du bon fonctionnement de l'entreprise

Le pouvoir de contrôle et de direction de l'employeur doit être exercé en lien avec les exigences du bon fonctionnement de l'entreprise. En appliquant par analogie les propos du juge Lebel dans l'arrêt *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*[124], il apparaît qu'un employeur qui décide d'exercer une surveillance de l'utilisation d'Internet de ses employés doit chercher à assurer le bon fonctionnement de l'entreprise :

> « Ainsi, il faut d'abord que l'on retrouve un lien entre la mesure prise par l'employeur et les exigences du bon fonctionnement de l'entreprise ou de l'établissement en cause. Il ne saurait s'agir d'une décision purement arbitraire et appliquée au hasard. L'employeur doit déjà posséder des motifs raisonnables avant

---

[123] Tels que les avocats, les médecins, pharmaciens, recteurs d'université ou gestionnaires de niveau supérieur. À ce sujet, voir M.-F. BICH, préc., note 113, aux pages 752 et 753.

[124] Préc., note 117.

de décider de soumettre son salarié à une surveillance. »[125]

À cet égard, tous les risques liés à l'utilisation d'Internet tels que mentionnés au premier chapitre sont susceptibles de nuire au bon fonctionnement de l'entreprise. En effet, que ce soit au niveau de la sécurité du système informatique, de la protection des informations confidentielles, des communications internes et externes, des relations entre collègues ou encore de la loyauté des employés, l'utilisation d'Internet par les employés peut nuire au bon fonctionnement de l'entreprise. Pour être légitime, la surveillance de l'utilisation d'Internet au travail, exercée par l'employeur en vertu de son pouvoir de direction et de contrôle, doit donc avoir un lien avec ces risques et avoir pour objet l'élimination ou la réduction d'un ou de plusieurs de ces risques.

Par ailleurs, les employés doivent respecter un certain nombre d'obligations en vertu de leur contrat de travail, lesquelles constituent des manifestations du lien de subordination qui caractérise la relation employeur-employé. Afin d'assurer le bon fonctionnement de l'entreprise, l'employeur a intérêt et a même le droit de vérifier que ses employés exécutent correctement leurs obligations, même lorsqu'ils utilisent l'accès Internet dans le cadre de leurs fonctions. Cette vérification vise également à assurer le bon fonctionnement de l'entreprise.

Les obligations principales de l'employé sont définies à l'article 2088 C.c.Q.[126]. L'obligation d'exécuter son travail avec prudence et diligence énoncée à l'article 2088 C.c.Q. consiste à exécuter le travail convenu avec compétence et en conformité avec les normes et directives établies par l'employeur, ce qui est convenu au contrat de travail ou, en l'absence, selon les règles d'usage du milieu de travail[127]. Bien que l'employé puisse contester ces normes et directives, c'est néanmoins l'employeur qui, en bout de ligne, décide de leur contenu et l'employé qui doit lui obéir sauf,

---

[125] *Id.*, 1089.

[126] C.c.Q., art. 2088 : « Le salarié, outre qu'il est tenu d'exécuter son travail avec prudence et diligence, doit agir avec loyauté et ne pas faire usage de l'information à caractère confidentiel qu'il obtient dans l'exécution ou à l'occasion de son travail. »

[127] *Dumoulin* c. *Gravel (Clinique de denturologie Rémi Gravel et Ass.)*, D.T.E. 2006T-26, AZ-50344142 (C.S.).

évidemment, en cas d'abus[128].

L'article 2088 C.c.Q. impose également l'obligation à l'employé d'agir avec loyauté envers son employeur et de ne pas faire usage d'information à caractère confidentiel qu'il obtient dans l'exécution de son travail. En vertu de son obligation de loyauté, laquelle s'apparente à une obligation de bonne foi, l'employé doit s'abstenir de tout acte malhonnête vis-à-vis de son employeur ou qui pourrait lui être dommageable[129]. Plus l'employé a de grandes responsabilités au sein de l'entreprise, plus son obligation de loyauté est grande[130].

L'obligation de loyauté dans le contexte de l'utilisation d'Internet implique notamment l'interdiction pour l'employé d'utiliser l'accès Internet à des fins personnelles de façon abusive, pouvant ainsi constituer du vol de temps[131], l'interdiction d'utiliser l'information appartenant à l'employeur pour son propre bénéfice[132], ou encore l'interdiction d'utiliser l'adresse électronique de l'entreprise de façon à porter atteinte à la réputation de son employeur[133].

Les risques liés à l'utilisation d'Internet au travail seraient grandement diminués si tous les employés respectaient leurs obligations légales de même que les diverses directives et politiques internes pouvant être établies par l'employeur quant à l'utilisation d'Internet au travail. Dans ce contexte, l'exercice d'une surveillance permettra à l'employeur de prévenir, détecter et faire cesser ces risques. Non seulement elle aura un effet dissuasif à l'égard des usages non-autorisés d'Internet, mais l'employeur pourra détecter et agir rapidement afin de les éliminer.

---

[128] *Centre hospitalier régional de Trois-Rivières (Pavillon St-Joseph) et Syndicat professionnel des infirmières et infirmiers de Trois-Rivières (Syndicat des infirmières et infirmiers Mauricie—Coeur-du-Québec)*, préc., note 113, par. 253.

[129] *Service d'entretien Serca* c. *Choquette*, D.T.E. 96T-699, J.E. 96-1239, AZ-96021446 (C.S.), p. 8; *Arpin* c. *Grenier*, préc., note 36, par. 33; et R. P. GAGNON, préc., note 112, par. 114, p. 80.

[130] *Banque de Montréal* c. *Kuet Leong Ng*, [1989] 2 R.C.S. 429, 438.

[131] *Supra*, p. 36.

[132] À titre d'illustration, voir : *D'Astous* c. *Sesno,* préc., note 90.

[133] À titre d'illustration voir : *Arpin* c. *Grenier*, préc., note 36.

2.1.1.3. Les pouvoirs complémentaires

2.1.1.3.1. LE POUVOIR DISCIPLINAIRE

Afin d'assurer le bon fonctionnement de l'entreprise, l'employeur dispose d'un pouvoir disciplinaire lui permettant d'appliquer des sanctions en cas de non respect des obligations de l'employé[134]. Ce pouvoir est considéré comme un corollaire nécessaire au pouvoir de contrôle et de direction du travail de l'employé et trouve d'ailleurs son fondement dans le pouvoir de contrôle et de direction de l'employeur[135].

L'employé qui ne respecte pas ses obligations, par exemple en utilisant Internet de façon abusive ou illégale durant les heures de travail, s'expose à des sanctions disciplinaires et peut voir sa responsabilité civile engagée[136]. Afin d'être en mesure d'exercer son pouvoir disciplinaire lorsque nécessaire, l'employeur doit pouvoir

---

[134] Julie LENFANT, *Le droit à la vie privée s'étend-il à l'utilisation du courriel par un employé dans le cadre de ses fonctions?*, Montréal, Faculté des études supérieures, 2000, en ligne : http://www.juriscom.net/uni/etd/04/priv01.pdf, p. 13; et R. PERREAULT, préc., note 111, à la page 75.

[135] *Cabiakman* c. *Industrielle-Alliance Cie d'Assurance sur la Vie* , préc., note 113, par. 45 : « Ce pouvoir trouve alors son fondement dans la nature même du contrat de travail et se déduit donc implicitement de l'art. 2085 C.c.Q. ou provient simplement de l'usage, sanctionné par l'art. 1434 C.c.Q. »

[136] Pour des illustrations de mesures disciplinaires prises pour une utilisation abusive ou illégale d'Internet, voir : *Syndicat canadien des communications, de l'énergie et du papier, section locale 522 et C.A.E. Électronique ltée,* préc., note 95; *Bell Canada et Association canadienne des employés de téléphone*, [2000] R.J.D.T. 358, D.T.E. 2000T-254 (T.A.); *Commission des normes du travail* c. *Bourse de Montréal inc.*, [2002] R.J.Q. 807 (C.Q.); *Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada*, [2003] R.J.D.T. 468, D.T.E. 2003T-89 (T.A.); *Blais et La Société des Loteries Vidéos du Québec Inc.*, [2003] R.J.D.T. 261, D.T.E. 2003T-178 (C.R.T.); *Syndicat de professionnelles et professionnels du gouvernement du Québec et Québec (Ministère du Revenu),* D.T.E. 2003T-582 (T.A.); *Fairmont Le Reine Élizabeth et Syndicat des travailleuses et travailleurs de l'Hôtel Le Reine Élizabeth (C.S.N.),* préc., note 97; *Syndicat des employés de bureau de Thetford Mines et Thetford Mines (Ville de),* préc., note 97; *Belisle et Municipalité de Rawdon*, 2005 QCCRT 0453, D.T.E. 2005T-777; *Syndicat canadien de la fonction publique, section locale 4140 et Centres jeunesse de l'Outaouais*, préc., note 97; *Pratt & Whitney Canada et Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleuses et travailleurs du Canada (TCA-Canada)*, D.T.E. 2005T-212 (T.A.); *Syndicat des spécialistes et professionnels d'Hydro-Québec, section locale 4250 (SCFP-FTQ) et Hydro-Québec*, préc., note 96; *Syndicat des employés municipaux de Beloeil (SCFP) et Beloeil (Ville de)*, préc., note 97; *Montour Ltée et Syndicat des employés et employés de la Cie Montour (CSN)*, préc., note 97; *Collège Ahuntsic* c. *Syndicat du personnel de soutien du Collège Ahuntsic*, préc., note 97; *Gilles et Ciba Spécialités chimiques Canada Inc.*, 2008 QCCRT 0134, D.T.E. 2008T-330; *Syndicat du personnel de soutien de la Seigneurie des Mille-Îles (CSN) et Commission scolaire de la Seigneurie-des-Mille-Îles*, D.T.E. 2008T-149 (T.A.); et *Syndicat de la fonction publique du Québec – Fonctionnaires et Québec (Ministère de l'Emploi et de la Solidarité sociale)*, préc., note 97. Pour un répertoire des mesures disciplinaires prises pour une utilisation abusive ou illégale d'Internet, voir : Sylvain LEFEBVRE, « Naviguer sur Internet au travail : et si on nageait en eaux trouble? », dans S.F.P.B.Q., vol. 293, *Développements récents en droit du travail (2008)*, Cowansville, Éditions Yvon Blais, aux pages 51 et suiv.

vérifier que ses employés respectent bien leurs obligations, exécutent leur travail selon ce qui a été convenu au préalable, respectent les politiques internes de l'entreprise et sont loyaux envers l'entreprise[137]. L'exercice de la surveillance de l'utilisation d'Internet est un moyen d'assurer cette vérification.

2.1.1.3.2. LE POUVOIR RÉGLEMENTAIRE ET NORMATIF

Une autre contrepartie au pouvoir de direction et de contrôle de l'employeur se retrouve dans son pouvoir réglementaire et normatif qui lui permet d'élaborer des règles s'imposant à tous les employés[138]. Ceux-ci ont l'obligation de respecter ces règles et directives adoptées par leur employeur, à moins évidemment qu'elles aillent à l'encontre de l'ordre public, mettent leur santé ou leur sécurité en danger, ou constituent une intrusion injustifiée dans leur vie privée[139].

C'est en vertu de son pouvoir réglementaire et normatif que l'employeur adoptera des politiques ou des directives régissant l'utilisation d'Internet au travail, ou prévoyant qu'une surveillance de l'utilisation d'Internet sera effectuée afin de vérifier, par exemple, la qualité et la quantité du travail des employés. Si l'employé refuse de s'y conformer sans motif raisonnable, il commettra alors un acte d'insubordination pouvant mener à l'imposition de mesures disciplinaires par l'employeur.

De telles politiques ou directives ont été considérées dans plusieurs décisions impliquant une mauvaise utilisation d'Internet au travail, à titre de facteur d'appréciation de la faute de l'employé[140]. Lorsqu'une telle politique est adoptée par

---

[137] K. DELWAIDE, préc., note 53, p. 14 : « Ces obligations sont à la base du pouvoir général de l'employeur de diriger et de contrôler son entreprise, droit qui inclut celui de surveiller le travail de ses employés. »

[138] J. LENFANT, préc., note 134, p. 13.

[139] *Dumoulin c. Gravel (Clinique de denturologie Rémi Gravel et Ass.)*, préc., note 127, par. 44.

[140] Voir notamment : *Syndicat canadien des communications, de l'énergie et du papier, section locale 522 et C.A.E. Électronique ltée*, préc., note 95; *Blais et La Société des Loteries Vidéos du Québec Inc.*, préc., note 136; *Syndicat canadien de la fonction publique, section locale 4140 et Centres jeunesse de l'Outaouais*, préc., note 97; *Syndicat du personnel de soutien de la Seigneurie des Mille-Îles (CSN) et Commission scolaire de la Seigneurie-des-Mille-Îles*, préc., note 136; et *Syndicat de la fonction publique du Québec – Fonctionnaires et Québec (Ministère de l'Emploi et de la Solidarité sociale)*, préc., note 97.

l'employeur et que l'employé, qui en a eu connaissance, contrevient aux règles qui y sont mentionnées, les tribunaux sont plus enclins à considérer que l'employé a contrevenu à ses obligations et que la mesure disciplinaire est justifiée dans les circonstances.

2.1.2. Le droit de propriété

2.1.2.1. L'approche fondée sur le droit de propriété de l'employeur

Une certaine approche en matière de surveillance de l'utilisation d'Internet au travail considère que la propriété de l'employeur, tant au niveau du système informatique que de l'accès à Internet, fonde son droit de surveillance. Cette approche, qui a été suivie à quelques reprises aux États-Unis[141], se décrit comme suit :

> « The property approach focuses on the fact that employers own the workplace including the resources that employees may be using for private purposes, such as computers and telephones. As a result of this ownership, employer are free to dictate to employees the manner in which such resources are used and employees only have privacy rights, or more accurately expectation of privacy, to the extent that employer policies allow. »[142]

Suivant cette approche, l'employeur a le droit de fouiller le système informatique comme toute autre propriété de la compagnie et c'est l'employeur qui décide ou non d'accorder une vie privée à ses employés dans le cadre de l'utilisation d'Internet au

---

[141] Voir notamment : *McLaren* v. *Microsoft Corp.*, 1999 WL 339015 (Tex.App.-Dallas); *Smyth* v. *Pillsbury Co.*, 914 F. Supp. 97 (U.S. Dist. Ct. E.D. Penn. 1996); *Garrity* v. *John Hancock Mut. Life Ins. Co.*, Civ. Act. No. 00-12143-RWZ, 2002 U.S.Dist. Lexis 8343 (D. Mass., May 7, 2002); et *Thygueson v. US Bancorp*, No. CV-03-467-ST, 2004, WL 2066746 (D.OR. Sept. 15, 2004). Pour une analyse approfondie de l'approche américaine en matière de surveillance de l'utilisation d'Internet fondée sur le droit de propriété de l'employeur, voir : Karen ELTIS, « The Emerging American Approach to E-Mail Privacy in the Workplace : Its Influence on Developing Case Law in Canada and Israël : Should Others Follow Suit? » (2002-2003) 24 *Comp. La. L. & Pl'y J.* 487, aux pages 499 et suiv.; Karen ELTIS, « La surveillance du courrier électronique en milieu de travail : le Québec succombera t-il à l'influence de l'approche américaine », (2006) 51 *R.D. McGill* 475, en ligne : http://lawjournal.mcgill.ca/documents/1224865238_Eltis.pdf, aux pages 483 et suiv.; et Vance LOCKTON et Richard S. ROSENBERG, *A preliminary Exploration of Workplace Privacy Issues in Canada*, report submitted to the Office of the Privacy Commissioner of Canada, University of British Columbia, April 10th, 2006, en ligne: http://www.cs.ubc.ca/~lockton/workplace.pdf, p. 40 et suiv.

[142] Avner LEVIN, Mary FOSTER, Mary Jo NICHOLSON et Tony HERNANDEZ, « Under the Radar? The Employer Perspective on Workplace Privacy », Ryerson University, Juin 2006, en ligne : https://www.theprivacynetwork.org/SSN/CurrentPrivacyIssues/WorkplaceandEmployment/Documents%20and%20Links/Ryerson%20Report%20-%20Under%20the%20Radar.pdf, p. 3.

travail[143].

Cette approche est notamment illustrée dans l'affaire américaine *Smyth* v. *Pillsbury Co.*[144], dans laquelle la Cour de Pennsylvanie a affirmé que l'employeur était justifié d'intercepter les communications Internet de son employé, et ce malgré les nombreuses représentations faites à l'effet que ces communications demeureraient confidentielles et privilégiées :

> « Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost. Significantly, the defendant did not require plaintiff, as in the case of an urinalysis or personal property search to disclose any personal information about himself. Rather, plaintiff voluntarily communicated the alleged unprofessional comments over the company e-mail system. We find no privacy interests in such communications. (...) Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments. »[145]

Dans la même veine, dans l'affaire de harcèlement sexuel *McLaren* v. *Microsoft Corp.*[146], la Cour d'Appel du Texas a conclu que l'employeur était justifié de fouiller dans les dossiers personnels informatiques de son employé et de décrypter son mot de passe afin de pouvoir accéder au contenu des messages électroniques. Selon la Cour, l'intérêt qu'a l'employeur de prévenir la circulation de messages inappropriés et la commission d'activités illégales sur son système de courrier électronique a préséance sur le droit à la vie privée de son employé[147].

---

[143] Marc-Alexandre POIRIER, « Employer Monitoring of the Corporate E-Mail System : How Much Privacy Can Employees Reasonably Expect? », (2002) 60 *U. Toronto Fac. L. Rev.* 85, à la page 96.

[144] Préc., note 141.

[145] *Id.*, p. 6 (nos soulignés).

[146] Préc., note 141.

[147] *Id.*, p. 5 : « Accordingly, the company's interest in preventing inappropriate and unprofessional comments, or even illegal activity, over its e-mail system would outweigh McLaren's claimed privacy interest in those communications. »

Au Canada, une approche similaire a été suivie à plusieurs reprises[148], notamment dans l'affaire de Colombie-Britannique *International Association of Bridge, Structure and Ornamental Ironworkers Local Union 97 and Officer and Technical Employees' Union Local 15*[149]. Dans sa décision, l'arbitre a invoqué le droit de propriété de l'employeur sur l'équipement informatique fourni à l'employé afin de justifier la surveillance au niveau du contenu des fichiers informatiques. L'arbitre a même affirmé que l'employé ne disposait d'aucune expectative de vie privée quant aux contenus se trouvant sur ces équipements[150].

À la lumière de ces différentes approches et illustrations, il est légitime de se demander si, en vertu du droit québécois, le droit de propriété de l'employeur sur les outils informatiques et l'accès Internet constitue un fondement de son droit de surveillance lui permettant ainsi d'invoquer ce droit pour justifier l'exercice d'une surveillance de l'utilisation d'Internet.

Cette question mérite une réponse négative, et ce, pour les motifs ci-après énoncés.

2.1.2.2. Non-application de l'approche du droit de propriété en droit québécois

Aucun tribunal québécois n'a encore justifié le droit de surveillance de l'employeur en se fondant sur le fait qu'il soit propriétaire des outils informatiques ou de l'accès Internet. Il apparaît par ailleurs qu'une telle approche serait incompatible avec la protection accordée aux droits fondamentaux des personnes en milieu de travail en vertu du droit québécois.

---

[148] Voir notamment : *Camosun College v. Canadian Union of Public Employees Local 2081*, [1999] B.C.C.A.A.A. 490, par. 25; *Telus Mobility and T.W.U. (Re)* (2001), 102 L.A.C. (4th) 239 (Can. Arbitration Board), 249 et 250; et *Milsom* v. *Corporate Computers Inc.* (2003), 17 Alta. L.R. (4th) 124 (ABQB), par. 46. Dans la doctrine, voir : K. ELTIS, « La surveillance du courrier électronique en milieu de travail : le Québec succombera t-il à l'influence de l'approche américaine », préc., note 141, à la page 479 : « Les tribunaux canadiens, pour leur part, semblent se rallier de plus en plus à une logique de la vie privée basée sur la propriété, aux dépens du droit à la vie privée des salariés. »

[149] [1997] B.C.C.A.A.A. 630.

[150] *Id.*, par. 64.

En effet, le droit civil québécois a pour principe que l'employé dispose d'une expectative de vie privée dans le lieu de travail, et ce, même s'il se trouve sur la propriété de l'employeur et utilise les biens de ce dernier. Cet aspect sera analysé plus en profondeur dans la section 2.2.1.2.2. du présent chapitre. Pour l'instant, nous soulignerons simplement les propos de l'auteur Morgan au soutien de notre prémisse à l'effet qu'en droit québécois, le droit de propriété de l'employeur ne peut fonder son droit de surveillance :

> « While the "physical plant", whether it be a computer system or a factory, may belong to the employer, still remains a private realm of the employee within the employer's property which the employer must respect. »[151]

L'importance de la vie privée dans le contexte d'une surveillance de l'utilisation d'Internet au travail se reflète d'ailleurs dans les propos de l'arbitre dans l'affaire *Syndicat canadien de la fonction publique, section locale 4140 et Centres jeunesse de l'Outaouais*[152] :

> « On ne peut reprocher à un employeur de ne pas avoir surveillé systématiquement un salarié à qui l'accès à Internet a été accordé à sa demande. [...]Dans un tel contexte, la confiance paraît être la règle alors que la surveillance de tout instant devrait être l'exception. »[153]

Bien qu'en 2004, l'arbitre Me René Turcotte, dans l'affaire *Syndicat des professionnelles et professionnels des affaires sociales du Québec (C.S.N.) et Institut de réadaptation en déficience physique de Québec*[154], semble avoir adopté l'approche fondée sur le droit de propriété, nous sommes d'avis que les principes énoncés dans cette décision méritent quelques nuances et rectifications.

En effet, dans cette affaire, l'arbitre Turcotte s'est exprimé comme suit :

---

[151] Charles MORGAN, « Employer Monitoring of Employee Electronic Mail and Internet Use », (1999) 44 *R. D. McGill* 849, 890. Voir également : K. ELTIS., « La surveillance du courrier électronique en milieu de travail : le Québec succombera t-il à l'influence de l'approche américaine », préc., note 141, aux pages 493-495.

[152] Préc., note 97.

[153] *Id.*, p. 36 et 37.

[154] D.T.E. 2004T-924, AZ-50270443 (T.A.).

> « La jurisprudence et la doctrine (M[e] André Rousseau, dans *l'Alliance de la Fonction publique du Canada* et *Le Musée des Beaux Arts du Canada (DTE 2003T-89(T.A.)* ; Louise Côté Desbiolles dans l'affaire *Sylvain Blais* et *La Société des Loteries Vidéos du Québec Inc(DTE 2003T-178(C.R.T.)* ; C. Bruce, dans l'affaire *Local Union No. 97 of the International Association of Bridge, Structural and Ornamental Ironworkers (the «Employer»), and Office and Technical Employees' Union, Local 15 (the «Union») (Garanito Grievance), Re : Karni Garanito Grievance,* [1997] B.C.C.A.A.A. No. 630 Award no. A-360/97) sont très claires en ce qui a trait au droit pour un employeur de vérifier le contenu d'un ordinateur que l'employeur fournit à son salarié. Il est en preuve que les ordinateurs de MM. Gauthier et Dubois ne sont pas leur propriété personnelle, mais bien un instrument de travail mis à leur disposition pour effectuer leur travail, pour l'utiliser uniquement à des fins professionnelles. »[155]

À la lecture de ces propos, il semble que le droit de propriété de l'employeur puisse fonder le droit de surveillance au Québec. Or, l'analyse des décisions québécoises citées par l'arbitre de même que de la jurisprudence en matière de surveillance électronique traditionnelle démontre que l'arbitre Turcotte a confondu les fondements du droit de surveillance avec les facteurs permettant d'établir l'expectative raisonnable de vie privée de l'employé.

En droit québécois, à la lumière des affaires *Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada*[156] et *Blais et La Société des Loteries Vidéos du Québec Inc.*[157], le fait que l'employeur soit propriétaire des outils informatiques et de l'accès Internet n'est qu'un des facteurs ayant pour effet de réduire l'expectative raisonnable de vie privée de l'employé à l'égard des activités menées au travail plutôt qu'un fondement du droit de la surveillance.

En effet, dans l'affaire *Blais et La Société des Loteries Vidéos du Québec Inc.*[158], la Cour n'affirme pas que l'employeur était justifié de fouiller le contenu de l'ordinateur de l'employé du fait que l'ordinateur, les logiciels et l'accès à Internet fournis à l'employé lui appartenaient. La propriété de l'employeur n'est qu'un des facteurs

---

[155] *Id.*, par. 293.

[156] Préc., note 136, 480 et 481.

[157] Préc., note 136, par. 94-97.

[158] *Id.*

considérés par la commissaire afin de conclure que l'employé ne pouvait raisonnablement s'attendre, en l'espèce, à ce que ses courriels et le contenu de son ordinateur demeurent privés :

> « En l'espèce, Sylvain Blais pouvait-il raisonnablement s'attendre à ce que ses courriels et le contenu de son ordinateur restent privés? La Commission doit répondre par la négative, compte tenu des éléments suivants. L'employeur fournit l'ordinateur, les logiciels et l'accès Internet afin que l'employé s'en serve dans le cadre de ses fonctions. (...) C'est dire que Sylvain Blais ne pouvait ignorer que le contenu des outils que la SLVQ mettait à sa disposition relevait davantage de sa vie professionnelle que de sa vie privée. Il ne pouvait ignorer, non plus, que les gestionnaires de réseau avaient accès à ce contenu, eux qui n'ont pas manqué de l'aviser, à plusieurs reprises, que ses courriels ou les sites qu'il visitait sur le Net n'étaient pas acceptables. (...) Tout ceci pour dire qu'en aucun moment le plaignant pouvait-il prétendre au caractère privé de ses échanges. Il faut en conséquence rejeter sa demande qu'ils soient exclus de la preuve parce que violant son droit au respect de sa vie privée. »[159]

Le même genre d'approche avait été adopté par la Cour d'appel dans l'affaire *Roy* c. *Saulnier*[160] en matière d'écoute téléphonique. En l'espèce, la propriété de l'employeur sur l'appareil téléphonique n'a pas été considérée comme justifiant l'interception les communications téléphoniques de l'employé. La propriété de l'employeur a plutôt été considérée comme l'un des éléments faisant en sorte que l'employé ne pouvait raisonnablement s'attendre à ce que ses conversations d'affaires durant les heures de travail demeurent privées.

L'approche fondée sur le droit de propriété est incompatible avec la façon dont les relations de travail sont aujourd'hui généralement menées et découle d'une vieille conception des droits de l'employeur basée sur le concept de propriété privée. Le caractère erroné de cette approche ressort d'ailleurs clairement des propos de l'auteur Marc-Alexandre Poirier[161] :

---

[159] *Id.*, par. 94-97. Voir également *R.* c. *Tremblay*, J.E. 2001-1310, AZ-01031335 (C.Q.), p. 6, conf. par B.E. 2003BE-315 (C.A.).

[160] [1992] R.J.Q. 2419 (C.A.).

[161] M.-A. POIRIER, préc., note 143.

> « The fallacy of this conception is appropriately illustrated by the following rhetorical question: "If I use a (company pen) to write a letter to my wife, does this mean that (my employer) can read the letter? (P. Zimmerman, 1996) »[162]

Par conséquent, au Québec, le droit de propriété de l'employeur à l'égard des outils informatiques fournis à ses employés ne fonde pas son droit de surveillance de l'utilisation d'Internet au travail. L'employeur a le droit de surveiller l'utilisation d'Internet au travail en vertu de son droit de direction et de contrôle, et non en vertu de son droit de propriété.

Notre position est d'autant plus renforcée par le fait qu'aux États-Unis, les tribunaux semblent de plus en plus enclins à reconnaître qu'un employé puisse jouir d'une expectative raisonnable de vie privée dans le cadre de l'utilisation d'Internet au travail, et ce, même s'ils utilisent les outils informatiques appartenant à l'employeur[163]. L'approche basée sur le droit de propriété serait donc en déclin aux États-Unis.

Maintenant, tel que nous le verrons dans la prochaine section, le droit de surveillance de l'employeur n'est pas un droit absolu et son exercice est sujet à certaines conditions découlant des limites imposées par les droits des personnes qui sont surveillées, que ce soit les employés ou les tiers impliqués.

2.2. Les limites du droit de surveillance de l'employeur

Tel que nous l'avons vu précédemment[164], en concluant un contrat de travail, un employé consent en quelque sorte à se placer en situation d'inégalité vis-à-vis de son employeur. Toutefois, en consentant à cette subordination, l'employé ne consent pas à n'importe quel abandon de liberté ou en d'autres mots ne renonce pas à la protection

---

[162] *Id.*, 96.

[163] À titre d'illustration, voir : *United States* v. *Angevine*, 281 F.3d 1130 (10th Cir. 2000); *Leventhal* v. *Knapek*, 266 F.3d 64 (2d Cir. 2001); *United States* v. *Slanina*, 283 F.3d, 670 (5th Cir. 2002); *United States* v. *Long*, 64 M.J. 57 (C.A.A.F.. 2006); et *United States* v. *Ziegler*, 497 F.3d. 890 (9th Cir. 2007).

[164] *Supra*, p. 44.

de ses droits fondamentaux, tel que souligné par l'auteur Gérard Lyon-Caen[165] :

> « Contre le salaire, le travailleur échange une prestation des services, qui seront définis par l'employeur, mais qui laissent intact un noyau dur qui correspond à ce qui, à une époque donnée, et dans une civilisation donnée, constitue l'idée qu'on se fait de la liberté humaine. »[166]

Par conséquent, le droit de surveillance de l'employeur est limité par les droits des personnes surveillées. L'employeur qui, dans l'exercice de la surveillance de l'utilisation d'Internet, dépasse ces limites, risque non seulement de se voir condamné à des dommages-intérêts, mais risque également, dans le cas d'un grief disciplinaire, de se voir refuser la production en preuve des résultats de sa surveillance en vertu de l'article 2858 C.c.Q.

Bien qu'aucun tribunal québécois n'ait encore conclu à l'illégalité d'une surveillance de l'utilisation d'Internet au travail, ils ont néanmoins, à quelques reprises, dû évaluer cette légalité au regard des droits des personnes surveillées[167]. Il est donc nécessaire, afin de s'assurer que la surveillance est exercée en toute légalité, de bien comprendre la portée et l'étendue des limites du droit de surveillance de l'employeur.

Les limites au droit de surveillance de l'employeur se présentent en deux volets, soit le droit à la vie privée des personnes surveillées et le droit à des conditions de travail justes et raisonnables. Nous verrons dans la présente section, les diverses dispositions législatives qui viennent établir ces limites et la façon dont ces limites sont interprétées lorsqu'elles viennent en conflit avec un droit de surveillance,

---

[165] Gérard LYON-CAEN, *Les libertés publiques et l'emploi*, Rapport pour le ministre du Travail, de l'Emploi et de la Formation professionnelle, Rapport officiel, Paris, La documentation française, 1992.

[166] *Id.*, p. 154. Voir également : *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.) c. Trudeau*, préc., note 117, 1088 : « La relation de dépendance dans l'exécution du travail ne permet pas d'induire un consentement du salarié au sens de l'article 35 C.c.Q., à toute atteinte à sa vie privée. »

[167] Voir notamment : *Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada*, préc., note 136; *Blais et La Société des Loteries Vidéos du Québec Inc.*, préc., note 136; et. À l'égard de la légalité d'une fouille exercée par l'employeur quant au contenu de l'ordinateur de travail d'un employé, voir : *Syndicat des professionnelles et professionnels des affaires sociales du Québec (C.S.N.) et Institut de réadaptation en déficience physique de Québec*, préc., note 154; et *Ghattas* c. *École nationale de théâtre du Canada*, [2006] R.J.Q. 852, J.E. 2006-644 (C.S.).

particulièrement dans le contexte de l'utilisation d'Internet au travail.

2.2.1. Le droit à la vie privée des personnes surveillées

2.2.1.1. Généralités

La principale limitation au droit de surveillance des employeurs découle du droit à la vie privée et à la protection des renseignements personnels des personnes surveillées[168]. En effet, dans l'arrêt *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*[169], la Cour d'appel a affirmé qu'« [u]ne procédure de surveillance et de filature représente (...), à première vue, une atteinte à la vie privée »[170]. Par analogie, il apparaît donc que la surveillance de l'utilisation d'Internet peut donc constituer une atteinte à la vie privée des employés.

Voyons maintenant comment le droit à la vie privée est protégé par la loi.

2.2.1.1.1. LA PROTECTION LÉGISLATIVE DE LA VIE PRIVÉE

La vie privée est protégée par plusieurs lois, tant au niveau international[171], provincial ou fédéral. Dans ce contexte, il est nécessaire pour un employeur de connaître les nombreuses dispositions qui viennent limiter son droit de surveillance, plus particulièrement au niveau fédéral et provincial.

2.2.1.1.1.1. *Charte canadienne des droits et libertés*

La Charte canadienne ne comporte pas de disposition expresse protégeant la vie privée des individus. Le droit à la vie privée découle plutôt de l'interprétation

---

[168] R. PERREAULT, préc., note 111, à la page 85.

[169] Préc., note 117.

[170] *Id.*, 1088.

[171] Au niveau international, voir *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, 4 novembre 1950, S.T.E. n° 5 (entrée en vigueur le 3 septembre 1953); *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, 28 janvier 1981, S.T.E. n° 108; *Déclaration universelle des droits de l'homme*, Rés. A.G. 217 (III), Doc. off. A.G. N.U., 3e sess., supp. n° 13, Doc. N.U. A/810 (1948); *Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontaliers de données à caractère personnel*, 23 septembre 1980; et *Pacte international relatif aux droits civils et politiques*, 16 décembre 1966, (1976) 999 R.T.N.U. 171.

jurisprudentielle de ses articles 7[172] et 8[173].

Le droit à la liberté tel que garanti à l'article 7 de la Charte canadienne implique notamment le droit pour chaque personne de disposer d'une certaine marge d'autonomie personnelle lui permettant de prendre des décisions sur des aspects privés qui la concernent[174]. On peut penser par exemple au droit pour une femme de décider d'élever un enfant seule, du choix du lieu de résidence[175], ou encore du choix des parents quant aux soins médicaux administrés à leurs enfants[176]. Cette marge d'autonomie personnelle est essentielle au bien-être de chaque personne et constitue l'un des fondements de la notion de vie privée. Une personne peut donc réclamer le droit de ne pas être importuné par l'État ou de contrôler la divulgation des renseignements personnels qui la concernent en vertu de cette disposition[177].

Par ailleurs, une fouille, une perquisition ou une saisie abusive au sens de l'article 8 de la Charte canadienne peut porter atteinte à la vie privée d'un individu[178]. Selon la Cour Suprême du Canada, l'article 8 de la Charte canadienne a pour objet de protéger les particuliers contre les intrusions injustifiées de l'État dans leur vie privée et doit être interprétée largement pour réaliser cette fin[179]. Dans ce contexte, les tribunaux ont reconnu à plusieurs reprises que la surveillance électronique clandestine d'un particulier était directement visée par cette disposition et pouvait porter atteinte à la

---

[172] *Charte canadienne*, art. 7 : « Chacun a droit à la vie, à la liberté et à la sécurité de sa personne; il ne peut être porté atteinte à ce droit qu'en conformité avec les principes de justice fondamentale. »

[173] *Charte canadienne*, art. 8 : « Chacun a droit à la protection contre les fouilles, les perquisitions et les saisies abusives. »

[174] *R.* c. *Beare*, [1988] 2 R.C.S. 387, 412; *R.* c. *Morgantaler*, [1988] 1 R.C.S. 30, 36; *Rodriguez* c. *Colombie-Britannique (Procureur général)*, [1993] 3 R.C.S. 519, 588; *Godbout* c. *Ville de Longueuil*, [1997] 3 R.C.S. 844, par. 98.

[175] *Godbout* c. *Ville de Longueuil*, préc., note 174.

[176] *B. (R.)*. c. *Children's Aid Society of Metropolitan Toronto*, [1995] 1 R.C.S. 315.

[177] Richard LANGELIER, « La protection de la vie privée par la Commission d'accès à l'information : quelle vie privée? Quelle protection? En fonction de quels intérêts? », dans S.F.P.B.Q., vol. 233, *Développements récents en droit de l'accès à l'information (2005)*, Éditions Yvon Blais, Cowansville, 2005, p. 149, à la page 204.

[178] *Hunther* c. *Southam Inc.*, [1984] 2 R.C.S. 145; *R.* c. *Duarte*, [1990] 1 R.C.S. 30; et *R.* c. *Wong*, [1990] 3 R.C.S. 36.

[179] *R.* c. *Dyment*, [1988] 2 R.C.S. 417, 426.

Charte si elle n'était pas justifiée en vertu de l'article premier :

> « On peut difficilement concevoir une activité de l'État qui soit plus dangereuse pour la vie privée des particuliers que la surveillance électronique et qui, en conséquence, doive être plus directement visée par la protection de l'art. 8. »[180]

D'ailleurs, l'interception de communications téléphoniques privées[181], du courrier électronique[182] de même que la fouille du contenu d'un ordinateur[183], ont été reconnues comme pouvant porter atteinte aux articles 7 et 8 de la Charte canadienne.

Bien qu'aucun tribunal n'ait encore appliqué la Charte canadienne dans le contexte d'une surveillance de l'utilisation d'Internet au travail[184], les articles 7 et 8 peuvent s'appliquer à un employeur qui exerce une telle surveillance, sous réserve évidemment que ses activités soient soumises aux dispositions de la Charte canadienne.

En vertu de l'article 32 de la Charte canadienne, la Charte s'applique uniquement aux actions de l'État et ne peut être invoquée dans le cadre d'un litige privé n'ayant aucun lien avec les gouvernements fédéral ou provincial[185]. À première vue, la Charte canadienne ne s'applique donc qu'aux ministères et organismes fédéraux et provinciaux.

Toutefois, les tribunaux reconnaissent à l'article 32 de la Charte canadienne une portée « assez large pour englober toutes les entités qui sont essentiellement de nature

---

[180] *R.* c. *Duarte*, préc., note 178, 43.

[181] *R.* c. *Solomon*, [1996] R.J.Q. 1789 (C.A.).

[182] *R.* v. *Weir*, [1998] 8 W.W.R. 228, 59 Alta. L.R. (3d) 319 (ABQB).

[183] *R.* c. *Gauthier*, [1999] R.J.Q. 2103, J.E. 99-1521 (C.Q.); et *R.* c. *Tremblay*, préc., note 159.

[184] L'affaire *R.* c. *Tremblay,* préc., note 159, se rapproche toutefois sensiblement de la surveillance de l'utilisation d'Internet. Il s'agissait en l'espèce d'une fouille du contenu de l'ordinateur d'un employé qui avait été surpris à visionner de la pornographie infantile. Rien n'indique dans la décision que les photographies provenaient de l'utilisation d'Internet par l'employé.

[185] Charte canadienne, art. 32(1) : « La présente charte s'applique : *a*) au Parlement et au gouvernement du Canada, pour tous les domaines relevant du Parlement, y compris ceux qui concernent le territoire du Yukon et les territoires du Nord-Ouest; *b*) à la législature et au gouvernement de chaque province, pour tous les domaines relevant de cette législature. »

gouvernementale et son champ d'application ne se limite pas aux seuls organismes qui font officiellement partie de la structure gouvernementale fédérale ou provinciale »[186].

Pour savoir si la Charte canadienne s'applique à une institution autre que le parlement fédéral ou provincial, il faut que l'entité accomplisse des actes pouvant être qualifiés de gouvernementaux et non simplement de publics[187]. C'est dans ce contexte que les tribunaux ont par exemple statué que la Charte canadienne pouvait s'appliquer à certains actes du Barreau du Haut-Canada[188], au collège Douglas[189], au Conseil des gouverneurs[190] et à des municipalités[191].

2.2.1.1.1.1. *Les lois fédérales pour la protection des renseignements personnels*

Le Canada compte deux lois visant à protéger les renseignements personnels : la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*. Ces deux lois fournissent un code législatif de pratiques équitables à l'égard des organismes et entités qui collectent, utilisent, conservent et communiquent des renseignements personnels sur les particuliers.

Compte tenu que l'exercice d'une surveillance de l'utilisation d'Internet équivaut souvent à recueillir et à utiliser des renseignements personnels sur les employés, ces dispositions s'appliquent directement à l'employeur qui désire exercer une telle surveillance :

---

[186] *Godbout* c. *Ville de Longueuil*, préc., note 174, par. 47.

[187] *Id.*, par. 49.

[188] *Klein* v. *Law Society of Upper Canada*, (1985) 50 O.R. (2d) 118 (Ontario Superior Court of Justice, Divisional Court).

[189] *Douglas/Kwantlen Faculty Assn.* c. *Douglas College*, [1990] 3 R.C.S. 570.

[190] *Lavigne* c. *Syndicat des employés de la fonction publique de l'Ontario*, [1991] 2 R.C.S. 211.

[191] *Godbout* c. *Ville de Longueuil*, préc., note 174.

> « Surveiller les courriels et les visites des employés sur le Web équivaut à recueillir et à utiliser les renseignements personnels des employés. Ce ne sont pas tous les renseignements qui sont confidentiels, mais certains le sont. Les renseignements personnels recueillis risquent d'être sensibles, surtout si l'employeur permet en certaines circonstances l'utilisation du courriel ou de l'Internet à des fins personnelles, par exemple à la pause du midi. »[192]

L'alinéa 4(1)b) L.p.r.p.d.é. prévoit d'ailleurs expressément que la loi s'applique aux organisations qui recueillent des renseignements personnels concernant leurs employés.

La *Loi sur la protection des renseignements personnels* a été adoptée en 1982 et est entrée en vigueur le 1er juillet 1983. Elle s'applique à toute l'administration publique fédérale, soit les ministères et organismes fédéraux, à l'exception du Parlement, des tribunaux et des sociétés de la Couronne en compétition directe avec le secteur privé (notamment Via Rail et la Société Radio-Canada[193])[194].

Quant à la L.p.r.p.d.é., son champ d'application est un peu plus complexe. Lors de son entrée en vigueur le 1er janvier 2001, elle ne s'appliquait qu'aux entreprises ou organismes commerciaux menant des activités dans des ouvrages, installations, entreprises ou secteurs d'activités de compétence fédérale, notamment les télécommunications, la radiodiffusion, le camionnage, la marine marchande, les chemins de fer et les autres moyens de transport d'une province à l'autre ou d'un pays à l'autre, l'aviation, les banques, l'énergie nucléaire, et les activités connexes à la navigation maritime et à la marine marchande[195]. Elle s'appliquait aussi aux renseignements personnels des employés de ces entreprises, ainsi qu'à la vente, à la

---

[192] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Le respect de la vie privée à l'ère d'Internet*, extrait de l'allocution de George Radwanski, Centre des relations industrielles de l'Université de Toronto et Lancaster House Publishing, 5e Conférence annuelle sur l'arbitrage en relations de travail, Toronto, 2 novembre 2001, en ligne : http://www.privcom.gc.ca/speech/02_05_a_011102_f.asp, p. 6.

[193] *Décret liant certains mandataires de Sa Majesté pour l'application de la partie 1 de la Loi sur la protection des renseignements personnels et les documents électroniques,* DORS/2001-8.

[194] Les sociétés d'État fédérales sont assujetties à la loi par décret.

[195] La loi ne s'applique toutefois pas aux établissements fédéraux qui sont soumis à l'application de *Loi sur la protection des renseignements personnels.*

location ou au troc de renseignements personnels au-delà des frontières provinciales ou nationales par des organisations sous réglementation provinciale. Elle s'appliquait également aux activités commerciales d'entreprises dans les territoires.

Depuis le 1er janvier 2004, la L.p.r.p.d.é. s'applique à toutes les transactions commerciales au Canada, sauf dans les provinces qui ont mis en place une loi essentiellement similaire à la loi fédérale.

En effet, le gouvernement du Canada peut exempter des organisations ou des activités dans les provinces qui ont adopté une loi sur la protection de la vie privée jugée essentiellement similaires à la loi fédérale. Au Québec, la *Loi sur la protection des renseignements personnels dans le secteur privé* a été jugée essentiellement similaire à la loi fédérale[196] et par conséquent, la partie 1 de la L.p.r.p.d.é. ne s'applique pas aux organisations québécoises qui sont assujetties à la *Loi sur la protection des renseignements personnels dans le secteur privé*. Au Québec, la L.p.r.p.d.é. continue par ailleurs à s'appliquer aux installations, ouvrages, entreprises ou secteurs d'activités fédéraux à l'intérieur de la province de Québec, de même qu'à toute collecte, utilisation et communication transfrontalière dans le cadre d'activités commerciales.

La L.p.r.p.d.é. ne s'applique par ailleurs qu'aux transactions commerciales et non au milieu du travail. Elle ne vise donc pas les renseignements personnels des travailleurs employés par des entreprises relevant d'une compétence provinciale.

Il est important que les employeurs vérifient s'ils sont assujettis à l'une de ces lois, de façon à prendre les mesures nécessaires pour respecter les obligations qui en découlent. À défaut, l'employeur pourra se voir imposer des sanctions pénales et pourra être poursuivi par l'employé pour atteinte à la vie privée.

2.2.1.1.1.3. *Code criminel*

---

[196] *Décret d'exclusion visant des organisations de la province de Québec*, DORS, 20043-374.

Plusieurs seront tentés d'affirmer que la surveillance de l'utilisation d'Internet au travail, plus particulièrement lorsque l'employeur enregistre les communications Internet de l'employé ou grave le contenu de son disque dur, contrevient à l'article 184 C.cr.[197] qui interdit l'interception de communications privées, ou encore l'article 342.1 C.cr.[198] qui interdit l'interception d'une fonction d'ordinateur. Or, pour les motifs ci-après exposés, il est difficile de voir comment ces dispositions puissent s'appliquer dans le contexte d'une surveillance de l'utilisation d'Internet au travail.

Aux termes de l'article 183 C.cr., le terme « intercepter » s'entend notamment du « fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet », et le terme « communication privée » s'entend d'une « communication orale ou télécommunication [...] qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers ». L'article 184 sera donc difficilement applicable dans le contexte d'une surveillance de l'utilisation d'Internet qui consiste généralement à enregistrer les actes des employés, tel qu'énoncé dans l'affaire *Blais et La Société des Loteries Vidéos du Québec Inc.*[199] :

> « [L]'essentiel de la preuve provient de la récupération d'informations stockées, étant acquis que l'entreprise procède, tous les jours, à la copie et à l'archivage sur disque compact du contenu des disques durs de tous les ordinateurs. On ne peut certes pas parler, dans ces circonstances, d'une « communication » au sens strict du terme,

---

[197] C.cr., art. 184(1) : « Est coupable d'un acte criminel et passible d'un emprisonnement maximal de cinq ans quiconque, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, intercepte volontairement une communication privée. »

[198] C.cr., art. 342.1(1) : « Quiconque, frauduleusement et sans apparence de droit : a) directement ou indirectement, obtient des services d'ordinateur; b) au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, directement ou indirectement, intercepte ou fait intercepter toute fonction d'un ordinateur; c) directement ou indirectement, utilise ou fait utiliser un ordinateur dans l'intention de commettre une infraction prévue à l'alinéa a) ou b) ou une infraction prévue à l'article 430 concernant des données ou un ordinateur; d) a en sa possession ou utilise un mot de passe d'ordinateur qui permettrait la perpétration des infractions prévues aux alinéas a), b) ou c), ou en fait le trafic ou permet à une autre personne de l'utiliser, est coupable d'un acte criminel et passible d'un emprisonnement maximal de dix ans ou d'une infraction punissable sur déclaration de culpabilité par procédure sommaire. »

[199] Préc., note 136.

encore moins d'une « interception. »[200]

En effet, pour que l'article 184 C.cr. s'applique, l'employeur doit intercepter une communication en cours, en transit[201]. Cette disposition ne s'applique donc pas à la récupération de fichiers enregistrés sur le disque dur de l'employé ou sur le serveur de l'employeur[202] ou à la récupération de courriels sur la puce mémoire d'un appareil *Blackberry*[203]. Par conséquent, elle n'affecte pas vraiment le droit de l'employeur de surveiller l'utilisation d'Internet au travail.

De plus, pour que l'article 184 C.cr. s'applique, l'interception doit viser une communication qualifiée de « privée », c'est-à-dire que l'employé doit disposer d'une expectative raisonnable de vie privée à l'égard de la communication interceptée[204]. Dans ce contexte, elle n'affecte pas le droit d'un employeur d'intercepter les communications professionnelles effectuées par les employés dans le cours de leurs fonctions[205].

L'article 342.1 C.cr., quant à lui, énonce que quiconque, frauduleusement et sans apparence de droit, intercepte une fonction d'ordinateur au moyen d'un dispositif quelconque, est coupable d'un acte criminel ou d'une infraction. Cette disposition n'a pas encore été appliquée par un tribunal canadien en matière de surveillance de l'utilisation d'Internet au travail. Toutefois, cette disposition n'affecte pas vraiment le droit de l'employeur de surveiller l'utilisation d'Internet au travail, compte tenu qu'en général l'employeur qui exerce une telle surveillance agit de bonne foi ou croit

---

[200] *Id.*, par. 92.

[201] *R.* v. *Bahr*, [2006] A.J. No. 1776, 434 A.R. 1 (Alberta Provincial Court), par 42 : « This meaning of the term [intercept] means that the interference must be contemporaneous with the transmission between the sender and the receiver. »

[202] Par analogie avec les principes énoncés dans *R.* v. *Bahr*, préc., note 201.

[203] *R.* v. *Giles*, [2007] B.C.J. No. 2918 (British Columbia Supreme Court).

[204] Pour une analyse de l'expectative raisonnable de vie privée d'un employé dans ses communications Internet au travail, voir *infra*, p. 78 et suiv.

[205] Kris KLEIN et Vivian GATES, *Privacy in Employment: Control of Personal Information in the Workplace*, Toronto, Thompson Carswell, 2005, p. 57.

posséder le droit d'exercer cette surveillance[206].

2.2.1.1.1.4. *Charte québécoise des droits et libertés de la personne*

Au Québec, le droit au respect de la vie privée est protégé par un grand nombre de dispositions, ce qui démontre l'importance pour le législateur québécois de protéger la vie privée des individus : le *Code civil du Québec*, la Charte québécoise, la *Loi sur la protection des renseignements personnels dans le secteur privé* et la *Loi sur l'accès.*

Dans la Charte québécoise, la vie privée est protégée par l'article 5[207]. Cette disposition s'applique à un employeur québécois qui exerce une surveillance de l'utilisation d'Internet, sous réserve que l'employé dispose d'une expectative raisonnable de vie privée[208].

Par ailleurs, tel qu'il ressort des propos de la Cour d'appel dans l'arrêt *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*[209], il est important de noter que la jurisprudence concernant l'article 8 de la Charte canadienne demeure pertinente dans l'application de l'article 5 de la Charte québécoise, même si le litige ne vise pas une action gouvernementale :

> « Étant donné que les deux Chartes protègent essentiellement le même droit à la vie privée, il n'est pas surprenant de constater que les décisions concernant l'art. 5 de la Charte québécoise font souvent appel aux principes énoncés en vertu de l'art. 8 de la

---

[206] Par analogie avec les principes énoncés dans *R.* v. *Bahr*, préc., note 201; C. MORGAN, « Employer Monitoring of Employee Electronic Mail and Internet Use », préc., note 151, 878; et M. GEIST, préc., note 107, p. 23.

[207] Charte québécoise, art. 5 : « Toute personne a droit au respect de sa vie privée. »

[208] Par analogie avec les principes énoncés dans *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, [2001] R.J.Q. 1111, J.E. 2001-1055 (C.A.). L'article 5 de la Charte québécoise a d'ailleurs été invoquée dans l'affaire *Blais et La Société des Loteries Vidéos du Québec Inc.,* préc., note 136, mais la Commission des relations de travail a conclu que cette disposition n'avait pas été violée, compte tenu qu'en l'espèce, l'employé ne pouvait raisonnablement s'attendre à ce que ses courriels et le contenu de son ordinateur restent privés.

[209] Préc., note 208.

Charte canadienne. »[210]

Il est donc toujours possible d'invoquer les principes et interprétations découlant de l'article 8 de la *Charte canadienne* dans le cadre de l'application de l'article 5 de la Charte québécoise.

Au Québec, personne ni aucune organisation de compétence provinciale ne peut en fait se soustraire à la Charte. Les seules organisations qui échappent à l'application de la Charte québécoise sont les institutions de compétence fédérale telles que la fonction publique fédérale[211], les banques, les entreprises de télécommunications, les services de transport aérien, ferroviaire ou maritime[212]. En effet, tel qu'indiqué à l'article 55 de la Charte québécoise, celle-ci vise les matières qui sont de la compétence législative du Québec.

2.2.1.1.1.5. *Code civil du Québec*

Le *Code civil du Québec* reconnaît à son article 3 que toute personne est titulaire d'un certain nombre de droits fondamentaux, dont le droit à la vie privée.

De plus, aux articles 35 à 41 du *Code civil du Québec*, le législateur a prévu un certain nombre de dispositions visant à protéger la vie privée. L'article 35 C.c.Q. vient réitérer le droit de toute personne au respect de la vie privée et interdit que toute atteinte y soit portée, à moins d'obtenir le consentement de l'intéressé. De plus, l'article 36 C.c.Q. prévoit une liste non-exhaustive d'exemples d'atteintes à la vie privée d'une personne.

Par ailleurs, les articles 37 à 41 du *Code civil du Québec* prévoient un certain nombre de règles concernant la protection des renseignements personnels. Au même titre que

---

[210] *Id.*, par. 68.

[211] Celles-ci sont par ailleurs soumises à la Charte québécoise.

[212] Dans ces cas, c'est la *Loi canadienne sur les droits de la personne* qui s'applique. Cette loi, qui s'applique aux organismes privés de juridiction fédérale en vertu de son article 2, ne comporte toutefois pas de disposition spécifique protégeant la vie privée des personnes, son objectif étant principalement de protéger les personnes contre la discrimination.

les lois sur la protection des renseignements personnels, l'article 37 C.c.Q. s'applique directement à l'employeur qui, par le biais de la surveillance, recueille des renseignements personnels sur son employé ou sur des tiers[213].

Les dispositions du *Code civil du Québec* ont été invoquées dans deux décisions impliquant l'exercice d'une surveillance de l'utilisation d'Internet[214]. Elles ont par ailleurs été invoquées à plusieurs reprises dans le cadre de la surveillance vidéo[215] ou par écoute téléphonique[216]. Elles demeurent donc pertinentes à l'égard de l'exercice de la surveillance de l'utilisation d'Internet par un employeur québécois, dans la mesure où l'employé dispose d'une expectative raisonnable de vie privée à l'égard des activités surveillées.

2.2.1.1.1.6. *Lois québécoises sur la protection des renseignements personnels*

---

[213] C.c.Q., art. 37 : « Toute personne qui constitue un dossier sur une autre personne doit avoir un intérêt sérieux et légitime à le faire. Elle ne peut recueillir que les renseignements pertinents à l'objet déclaré du dossier et elle ne peut, sans le consentement de l'intéressé ou l'autorisation de la loi, les communiquer à des tiers ou les utiliser à des fins incompatibles avec celles de sa constitution; elle ne peut non plus, dans la constitution ou l'utilisation du dossier, porter autrement atteinte à la vie privée de l'intéressé ni à sa réputation. »

[214] *Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada*, préc., note 136; et *Blais et La Société des Loteries Vidéos du Québec Inc.*, préc., note 136.

[215] Décisions ayant conclu à une violation des dispositions du *Code civil du Québec* : *Unidindon inc. et Syndicat des travailleurs d'abattoir de volaille de St-Jean-Baptiste (C.S.N.)*, D.T.E. 2000T-368 (T.A.), Requête en révision judiciaire rejetée, [2000] R.J.Q. 2064, J.E. 2000-1273(C.S.), conf. par D.T.E. 2001T-206 (C.A.); *Syndicat canadien des communications, de l'énergie et du papier et Induspac, division Corrugué inc.*, [2000] R.J.D.T. 837, D.T.E. 2000T-507 (T.A.); *Amziane* c. *Bell Mobilité*, D.T.E. 2004T-849, J.E. 2004-1702 (C.S.); et *Syndicat de l'enseignement des Deux Rives (SEDR-CSQ) et Commission scolaire des Navigateurs*, D.T.E. 2007T-516, AZ-50433953 (T.A.). Décisions ayant conclu que l'employeur, dans l'exercice de sa surveillance, n'avait pas enfreint les dispositions du *Code civil du Québec* : *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 117; *Syndicat de l'industrie du journal du Québec inc. (distribution) (CSN) et Presse ltée (La)*, D.T.E. 2000T-1167 (T.A.); *Syndicat démocratique des employés de commerce Saguenay-Lac-St-Jean et Potvin & Bouchard inc.*, [2006] R.J.D.T. 221, D.T.E. 2006T-75 (T.A.); *Syndicat des travailleurs unis du Québec — STUQ (FTQ) et Pomatek inc.*, D.T.E. 2007T-784, AZ-50448279 (T.A.); et *Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleuses et travailleurs du Canada et BMW Canbec*, D.T.E. 2007T-697, AZ-50441929 (T.A.).

[216] Décisions ayant conclu à une violation des dispositions du *Code civil du Québec* : *Srivastava* c. *Hindu Mission of Canada (Quebéc) Inc.*, préc., note 208; Décisions ayant conclu que l'employeur, dans l'exercice de sa surveillance, n'avait pas enfreint les dispositions du *Code civil du Québec* : *Ste-Marie* c. *Placements JPM Marquis inc.*, [2005] R.R.A. 295, J.E. 2005-711 (C.A.); *Bellefeuille* c. *Morisset*, [2007] R.J.Q. 796, J.E. 2007-899 (C.A.); et *Syndicat des salariées et salariés de La Survivance et La Survivance*, [2006] R.J.D.T. 1657, D.T.E. 2006T-875 (T.A.).

Quant aux activités de collecte, d'utilisation, de détention et de communication de renseignements personnels, la Loi sur le secteur privé et la Loi sur l'accès prévoient une panoplie de règles similaires aux lois fédérales qui régissent la collecte, l'utilisation et la communication de renseignements personnels par des organisations. Ces deux lois s'appliquent directement à l'employeur qui, par le biais de la surveillance de l'utilisation d'Internet, traite des renseignements personnels sur ses employés ou sur des tiers.

La Loi sur le secteur privé s'applique aux entreprises privées de compétence provinciale[217], alors que la Loi sur l'accès s'applique aux organismes publics et aux ordres professionnels québécois[218].

Par ailleurs, les deux lois québécoises sur la protection des renseignements personnels contiennent plusieurs dispositions qui, bien que formulées différemment, ont sensiblement leur équivalent dans les lois fédérales mentionnées précédemment. La façon dont ces dernières sont interprétées peut donc également servir de guide pour l'application des dispositions québécoises[219].

2.2.1.1.2. LA NOTION DE « VIE PRIVÉE » ET LE CRITÈRE DE L'ATTENTE RAISONNABLE DE VIE PRIVÉE

Pour déterminer si un geste ou un acte porte atteinte à la vie privée, il est nécessaire de déterminer si la divulgation ou l'intrusion porte sur un élément de la vie privée, et donc de circonscrire la notion de « vie privée »[220]. Bien que celle-ci ait fait l'objet de

---

[217] Cette loi ne s'applique donc pas aux entreprises de juridiction fédérale. À cet égard, voir : *Air Canada* c. *Constant*, [2003] C.A.I. 710, J.E. 2003-1799 (C.S.). Inscription en appel, 2003-10-02 (C.A.), 500-09-013818-034.

[218] Loi sur l'accès, art. 1 et 1.1.

[219] *Laforest* c. *Caisse de dépôt et placement du Québec,* [2004] C.A.I. 31 (C.A.I.), par. 39; Voir également : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Nouvelle loi, nouvelle époque*, Allocution de George Radwanski à la Conférence de l'Université de Toronto et Lancaster House sur les derniers développements en matière de vie privée au travail, Toronto, 6 avril 2001, en ligne : http://www.privcom.gc.ca/speech/02_05_a_010406_f.asp, p. 4.

[220] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Thémis, 1997, p. 11-26.

plusieurs interprétations par les tribunaux au fil du temps[221], il semble difficile d'en arriver à une définition qui fasse l'unanimité[222]. De plus, aucune loi québécoise ou canadienne ne comporte de définition formelle de cette notion.

Par ailleurs, il faut bien comprendre que cette notion a une portée différente dépendamment des contextes, des époques, des mœurs et des personnes[223]. Il s'agit d'une notion qui n'est pas fixe ni dans le temps ni dans l'espace et qui évolue continuellement.

La notion de vie privée, traditionnellement définie comme le droit d'être laissé seul[224], englobe aujourd'hui le fait de ne pas faire l'objet d'une surveillance, de ne pas être dérangé, épié ou sollicité, le droit à l'anonymat[225], au secret et à la confidentialité[226], de même que le droit de contrôler l'accès à sa personne et aux renseignements qui nous concernent[227].

Par ailleurs, pour circonscrire la vie privée et la protection qui lui est conférée, il faut prendre en compte un ensemble de facteurs liés au contexte dans lequel se trouve la personne à un moment déterminé, et apprécier les attentes raisonnables de cette personne quant à sa vie privée.

En effet, la protection de la vie privée garantie dans les diverses législations fédérales

---

[221] *R.* c. *Dyment*, préc., note 179, 429 et 430; *R.* c. *Duarte*, préc., note 178, 46; *R.* c. *Osolin*, [1993] 4 R.C.S. 595, 613-615; *Aubry* c. *Éditions Vice-Versa Inc.*, [1998] 1 R.C.S. 591, par. 51 et suiv.; et *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 117, 1087.

[222] R. PERREAULT, préc., note 111, à la page 87; et Édith DELEURY et Dominique GOUBAU, *Le droit des personnes physiques*, Cowansville, Les Éditions Yvon Blais, 1994, par. 167, p. 185.

[223] P. TRUDEL, F. ABRAN, K. BENYEKHLEF et S. HEIN, préc., note 220, p. 11-25.

[224] Samuel D. WARREN et Louis D. BRANDEIS, *The right to Privacy*, (1890) 4 *Harvard L.Rev.* 193, en ligne: http://www.abolish-alimony.org/content/privacy/Right-to-Privacy-Brandeis-Warren-1890.pdf.

[225] *Aubry* c. *Éditions Vice-Versa inc.*, préc., note 221.

[226] *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 117, 1087; Voir également E. DELEURY, D. GOUBAU, préc., note 222, p. 137; et R. PERREAULT, préc., note 111, à la page 87.

[227] *R.* c. *Dyment*, préc., note 179, 429 et 430; *R.* c. *Duarte*, préc., note 178, 46; *R.* c. *Osolin*, préc., note 221, 613-615; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La vie privée au travail à l'ère d'Internet*, préc., note 1, p. 2; et K. DELWAIDE, préc., note 53, p. 23.

et provinciales susmentionnées ne vise pas toutes les attentes en matière de vie privée. La protection ne vise que les attentes ou expectatives qualifiées de « raisonnables » de la personne visée, relativement à une activité ou à une information quelconque. Cela représente une distinction importante, particulièrement lorsqu'il s'agit d'évaluer la légalité d'une mesure de surveillance.

Le concept d' « expectative raisonnable de vie privée » ou d' « attente raisonnable de vie privée »[228] est apparu pour la première fois au Canada en 1982, dans l'arrêt *Hunther* c. *Southam*[229], dans le contexte de l'application de l'article 8 de la Charte canadienne :

> « La garantie de protection contre les fouilles, les perquisitions et les saisies abusives ne vise qu'une attente raisonnable. Cette limitation du droit garanti par l'art. 8, qu'elle soit exprimée sous la forme négative, c'est-à-dire comme une protection contre les fouilles, les perquisitions et les saisies "abusives", ou sous la forme positive comme le droit de s'attendre "raisonnablement" à la protection de la vie privée, indique qu'il faut apprécier si, dans une situation donnée, le droit du public de ne pas être importuné par le gouvernement doit céder le pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins et, notamment, d'assurer l'application de la loi. »[230]

Suite à l'arrêt *Hunther* c. *Southam Inc.*[231], la Cour suprême du Canada est venue préciser que l'appréciation du caractère raisonnable de l'attente devait se faire eu égard à l'ensemble des circonstances d'un cas particulier[232]. En effet, l'expectative raisonnable de vie privée varie selon le contexte. De plus, la Cour a insisté sur l'importance de l'existence d'une attente subjective en matière de vie privée, et sur l'importance du caractère raisonnable de l'attente sur le plan objectif[233].

Le concept de l'expectative raisonnable de vie privée est également appliqué en droit

---

[228] Les deux concepts ayant la même signification.

[229] Préc., note 178.

[230] *Id.*, 159.

[231] Préc., note 178.

[232] *R.* c. *Wong,* préc., note 178, 62; *R.* c. *Colarusso*, [1994] 1 R.C.S. 20, 54; et *R.* c. *Edwards*, [1996] 1 R.C.S. 128, par. 31.

[233] *R.* c. *Edwards*, préc., note 232, par. 45; et *R.* c. *M. (M.R.)*, [1998] 3 R.C.S. 393, par. 32.

québécois afin de déterminer si le droit à la vie privée tel que garanti par l'article 5 de la Charte québécoise et les dispositions du *Code civil du Québec* a été violé[234].

Pour apprécier le niveau d'expectative raisonnable de vie privée d'une personne ou d'un groupe donné dans une situation donnée, plusieurs facteurs doivent être pris en compte, que ce soit à l'égard du lieu, de la personne, de la propriété du bien ou du lieu ou de la nature des renseignements[235]. Tel que nous le verrons dans les prochaines sections, l'appréciation de ces différents facteurs dans des situations données, notamment en milieu de travail, peut mener à la conclusion que l'expectative raisonnable de vie privée des personnes est réduite, ou sinon même inexistante[236].

Nous allons donc maintenant analyser comment déterminer le niveau d'expectative de vie privée d'un employé qui se trouve sur le lieu de travail, et plus particulièrement lorsqu'il utilise Internet dans le cadre de son travail.

2.2.1.2. Le droit à la vie privée des employés

2.2.1.2.1. LA RECONNAISSANCE D'UN DROIT

En principe, les activités d'un employé dans l'exécution de ses fonctions ne relèvent pas de sa vie privée[237]. Cette thèse se fonde sur le lien de subordination qui caractérise le rapport entre l'employeur et l'employé et qui justifie une certaine ingérence par l'employeur dans la vie privée de l'employé :

---

[234] À titre d'illustration, voir : *Roy* c. *Saulnier,* préc., note 160; *Mascouche (Ville de)* c. *Houle*, [1999] R.J.Q. 1894 (C.A.); *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, préc., note 208; *Ste-Marie* c. *Placements JPM Marquis inc.*, préc., note 216; *Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada*, préc., note 136; et *Blais et La Société des Loteries Vidéos du Québec Inc.,* préc., note 136.

[235] Pour les facteurs d'appréciation établis en vertu de l'art. 8 de la Charte canadienne, voir : *R.* c. *Edwards*, préc., note 232, par. 45; et *R.* c. *M. (M.R.)*, préc., note 233, par. 31. Pour les facteurs d'appréciation établis en vertu de la Charte québécoise, voir : *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, préc., note 208, par. 68. Dans la doctrine, voir : R. LANGELIER, préc., note 177, à la page 197.

[236] François BLANCHETTE, *L'expectative raisonnable de vie privée et les principaux contextes de communications dans Internet*, thèse de maîtrise, Montréal, Faculté des études supérieures, 2001, en ligne : http://www.juriscom.net/documents/priv20040203.pdf, p. 31.

[237] *Société des alcools du Québec* c. *Syndicat des employés de magasins et de bureaux de la S.A.Q.*, [1983] T.A. 335, 341.

> « De façon générale, un salarié au travail loue ses services à un employeur qui a le droit de prendre les mesures qui s'imposent pour vérifier la nature et la qualité du travail fourni. À cette fin, rien ne lui interdit de surveiller le salarié pour s'assurer de la qualité de son travail et on ne peut certes pas prétendre que pendant le temps où le salarié effectue sa prestation de travail, on est toujours dans le strict domaine de la vie privée. »[238]

Ainsi, on reconnaît qu'en milieu de travail, l'expectative de vie privée de l'employé se voit réduite[239].

Toutefois, l'employé ne renonce pas implicitement à son droit à la vie privée en franchissant les portes de son lieu de travail. Tel qu'énoncé par la Cour d'appel dans l'arrêt *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*[240], « [l]a relation de dépendance dans l'exécution du travail ne permet pas d'induire un consentement du salarié, au sens de l'article 35 C.C.Q., à toute atteinte à sa vie privée »[241].

Il existe des circonstances où, même au travail, l'employé peut faire valoir son droit à la vie privée, limitant ainsi le droit d'ingérence de l'employeur[242]. Ce sera le cas notamment en matière de surveillance vidéo[243], de l'enregistrement des conversations

---

[238] *Id.*

[239] *Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada*, préc., note 136, 480.

[240] Préc., note 117.

[241] *Id.*, 1088. Voir également *R.* c. *Tremblay* (C.A.), préc., note 159, p. 2; *Syndicat des employées et employés professionnels et de bureau, section locale 57 et Caisse populaire St-Stanislas de Montréal*, [1999] R.J.D.T. 350, D.T.E. 99T-59 (T.A.), 364; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La vie privée au travail à l'ère d'Internet*, préc., note 1, p. 2; et Diane VEILLEUX, « Le droit à la vie privée – sa portée face à la surveillance de l'employeur », (2000) 60 *R. du B.* 1, 25.

[242] D. VEILLEUX, préc., note 241, 20; et Karl DELWAIDE, « La protection de la vie privée et les nouvelles technologies : l'accès au courrier électronique des employés par un employeur », dans S.F.P.B.Q., *Congrès annuel du Barreau du Québec (1997)*, Cowansville, Éditions Yvon Blais, p. 627, à la page 640.

[243] À titre d'illustration, voir : *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 117; *Syndicat de l'industrie du journal du Québec inc. (distribution) (CSN) et Presse ltée (La)*, préc., note 215; *Poulies Maska inc. et Syndicat des employés de Poulies Maska inc.*, D.T.E. 2001T-620, AZ-01141163 (T.A.); *Syndicat des employés municipaux de la Ville de Saguenay (CSN) et Saguenay (Ville de)*, D.T.E. 2005T-511 (T.A.); *Syndicat des travailleuses et travailleurs de la Fabrique Notre-Dame — CSN et Fabrique de la paroisse Notre-Dame*, D.T.E. 2006T-56 (T.A.); *Vifan Canada inc. et Syndicat des travailleuses et travailleurs de Vifan Canada inc. (CSN)*, D.T.E. 2007T-698, AZ-50445314 (T.A.); *Syndicat des travailleurs unis du Québec — STUQ (FTQ) et Pomatek inc.*, préc., note 215; *Syndicat de l'enseignement des Deux Rives (SEDR-CSQ) et Commission scolaire des Navigateurs*, préc., note 215; *Syndicat national des travailleurs des pâtes et papiers de Donnacona inc. (CSN) et Produits forestiers Alliance inc. (Bowater)*,

téléphoniques intervenues sur le lieu de travail[244], des examens médicaux exigés des employeurs[245] et des codes vestimentaires ou d'apparence personnelle imposés aux employés[246] . Il ne s'agit pas ici d'affirmer que dans chacune de ces situations, l'employé dispose d'une expectative de vie privée, chaque cas constituant un cas d'espèce. Par contre, les tribunaux ont déjà reconnu l'existence d'une expectative raisonnable de vie privée pour l'employé dans chacune de ces situations[247].

Les propos suivants de Georges Radwanski, ancien Commissaire à la vie privée du Canada, viennent d'ailleurs nous rappeler l'existence du droit à la vie privée en milieu

---

[2008] R.J.D.T. 958, D.T.E. 2008T-469 (T.A.); *Laplante* c. *Groupe de sécurité Garda inc.*, B.E. 2008BE-478 (C.Q.); et *Syndicat des employées et employés professionnels et de bureau, section locale 575 et Caisse Desjardins Thérèse-de-Blainville (D.D.)*, D.T.E. 2009T-170 (T.A.).

[244] À titre d'illustration, voir : *Roy* c. *Saulnier*, préc., note 160; *Mascouche (Ville de)* c. *Houle*, préc., note 234; *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, préc., note 208; *Ste-Marie* c. *Placements JPM Marquis inc.*, préc., note 216; *Bellefeuille* c. *Morisset*, préc., note 216; *Syndicat des employées et employés de techniques professionnelles et de bureau d'Hydro-Québec, section locale 2000 (SCFP/FTQ) et Hydro-Québec*, D.T.E. 2005T-881 (T.A.); et *Syndicat des salariées et salariés de La Survivance et La Survivance*, préc., note 216.

[245] À titre d'illustration, voir : *Québec (Ministère du Revenu) et Syndicat de la fonction publique du Québec (Gouvernement du Québec (Ministère du Revenu) et Syndicat de la fonction publique du Québec)*, D.T.E. 99T-645 (T.A.); *Syndicat des employées et employés professionnels et de bureau, section locale 57 et Caisse populaire St-Stanislas de Montréal*, préc., note 241; *Métallurgistes unis d'Amérique, section locale 9414 et Nettoyeur Shefford inc.*, D.T.E. 2000T-272 (T.A.); *Syndicat catholique des ouvriers du textile de Magog inc., section locale 10 et DIFCO Tissus de performance inc.*, [2000] R.J.D.T. 877 (T.A.); *Syndicat des travailleurs de Praxair (C.S.N.) et Praxair inc.*, D.T.E. 2002T-413 (T.A.); *Union des employées et employés de service, section locale 800 et Collège Marie de France,* [2004] R.J.D.T. 1284, D.T.E. 2004T-645 (T.A.); et *Syndicat des salariées et salariés de General Dynamics, produits de défense et systèmes tactiques — Canada inc. et General Dynamics*, D.T.E. 2008T-904 (T.A.).

[246] À titre d'illustration, voir : *Ville de Montréal* c. *Association des pompiers de Montréal Inc.*, D.T.E. 90T-323 (T.A.); et *Employés du transport local et industries diverses, section locale 931 et United Parcel Service Canada*, [2003] R.J.D.T. 1861, D.T.E. 2003T-1129 (T.A.), inf. par J.E. 2006-1121, D.T.E. 2006T-519 (C.S.).

[247] En matière de surveillance vidéo, voir : *Syndicat canadien des communications, de l'énergie et du papier et Induspac, division Corrugué inc.*, préc., note 215; *Unidindon inc. et Syndicat des travailleurs d'abattoir de volaille de St-Jean-Baptiste (C.S.N.)*, préc., note 215; *Amziane* c. *Bell Mobilité*, préc., note 215; *Syndicat de l'enseignement des Deux Rives (SEDR-CSQ) et Commission scolaire des Navigateurs*, préc., note 215; . En matière d'écoute téléphonique, voir : *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, préc., note 208. En matière d'examen médical, voir : *Québec (Ministère du Revenu) et Syndicat de la fonction publique du Québec (Gouvernement du Québec (Ministère du Revenu) et Syndicat de la fonction publique du Québec)*, préc., note 245; *Syndicat catholique des ouvriers du textile de Magog inc., section locale 10 et DIFCO Tissus de performance inc.*, préc., note 245; et *Syndicat des salariées et salariés de General Dynamics, produits de défense et systèmes tactiques — Canada inc. et General Dynamics*, préc., note 245. En matière d'apparence personnelle, voir : *Ville de Montréal* c. *Association des pompiers de Montréal Inc.*, préc., note 246.

de travail comme droit fondamental[248] :

> « Je crois que les employés ont un droit fondamental et inhérent à leur vie privée en milieu de travail. C'est aussi l'avis de juges et d'arbitres qui reconnaissent depuis longtemps que les employés ont des droits à la vie privée qui leur sont propres et qu'ils peuvent défendre. Cela vaut pour leurs communications personnelles, leurs casiers et tiroirs, leurs effets personnels, etc.
>
> C'est également un avis qui est appuyé autant par la *Loi sur la protection des renseignements personnels* que par la *Loi sur la protection des renseignements personnels et les documents électroniques*.
>
> Il est logique que le Parlement adopte des lois pour protéger la vie privée en milieu de travail. On ne laisse pas nos droits fondamentaux à la porte du bureau ou de l'usine comme on y laisserait son manteau. »[249]

À l'égard de l'utilisation d'Internet au travail, il est évident que les employés utilisent parfois cet outil de communication à des fins personnelles et qu'ils s'attendent, dans certaines circonstances, à ce que cette utilisation demeure privée. Reprenant les propos de l'arbitre dans l'affaire *Bell Canada et Association canadienne des employés de téléphone*[250], « [c]e serait faire l'autruche que de ne pas admettre que l'utilisation de l'Internet a pu servir quelquefois à des fins personnelles pour plusieurs employés »[251].

Par conséquent, lorsqu'il s'agit d'évaluer la légalité d'une surveillance exercée par un employeur, la première question que nous devons nous poser est la suivante : compte tenu de toutes les circonstances, l'employé pouvait-il raisonnablement s'attendre à ce que l'employeur considère ses communications électroniques ou ses activités Internet comme étant protégées par son droit à la vie privée?

L'arrêt québécois qui fournit le plus d'indications quant aux facteurs qui doivent être

---

[248] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La vie privée au travail à l'ère d'Internet*, préc., note 1.

[249] *Id.*, p. 2.

[250] *Bell Canada et Association canadienne des employés de téléphone*, préc., note 136.

[251] *Id.*, 366 : Voir également G. LASPROGATA, préc., note 108, par. 17.

pris en compte dans le contexte des communications au travail est l'arrêt *Srivastava c. Hindu Mission of Canada (Québec) Inc.*[252]. Dans cet arrêt, la Cour d'appel du Québec affirme que les différents facteurs à considérer dans l'appréciation des circonstances sont les suivants : (i) la présence de la personne visée au moment de la perquisition ; (ii) la possession ou contrôle du bien ou lieu faisant l'objet de la fouille ou perquisition ; (iii) la propriété du bien ou du lieu ; (iv) l'usage historique du bien ou de l'article ; (v) l'habilité à régir l'accès au lieu, y compris le droit d'en exclure autrui ; (i) l'existence d'une attente subjective en matière de vie privée ; et (vii) le caractère raisonnable de l'attente.

Bien que cet arrêt traite de l'expectative de vie privée à l'égard des conversations téléphoniques, il contient plusieurs principes qui peuvent s'appliquer par analogie dans le cadre de l'évaluation de l'expectative de vie privée dans l'utilisation d'Internet au travail.

Par ailleurs, dans le cadre de l'évaluation de l'expectative raisonnable de vie privée des employés qui utilisent Internet au travail, de nouveaux facteurs doivent être pris en considération. Internet offre un outil de communication et d'information ayant des particularités qui lui sont propres et qui entraînent une augmentation significative des contextes susceptibles de faire varier le niveau d'expectative raisonnable de vie privée des gens qui l'utilisent. Il faut donc tenir compte de facteurs additionnels propres aux nouvelles technologies de l'information et de la communication.

2.2.1.2.2. LA DÉTERMINATION DE L'EXPECTATIVE RAISONNABLE DE VIE PRIVÉE DES EMPLOYÉS DANS L'UTILISATION D'INTERNET AU TRAVAIL

La détermination du niveau d'expectative de l'employé permet de délimiter l'étendue du droit de surveillance que l'employeur peut exercer et la manière dont celle-ci doit être menée. Il est donc important qu'un employeur détermine le niveau d'expectative de vie privée de l'employé avant d'exercer une surveillance de l'utilisation d'internet

---

[252] Préc., note 208.

de ses employés, que celle-ci soit ponctuelle ou continue.

Si la surveillance est ponctuelle, si par exemple l'employeur décide, pour certaines raisons, de fouiller dans la boîte de courrier électronique d'un employé en particulier, l'employeur devra se demander si l'employé visé, lorsqu'il a reçu ou transmis les messages contenus dans la boîte de courrier électronique, pouvait raisonnablement s'attendre à ce qu'ils demeurent privés. Si par ailleurs l'employeur exerce une surveillance continue et permanente à l'égard de tous les employés de l'entreprise, l'analyse de l'expectative de vie privée devra être faite de manière plus globale, étendue à l'ensemble des employés.

S'il appert que le ou les employés ne disposent d'aucune expectative raisonnable de vie privée dans l'utilisation d'Internet au travail, l'employeur n'aura pas à remplir de critères pour restreindre le droit à la vie privée du ou des employés. Le cas échéant, les conditions d'exercice de la surveillance seront beaucoup moins sévères, sous réserve du droit des employés à des conditions de travail justes et raisonnables[253]. Si, par ailleurs, il appert que l'employé dispose d'une expectative raisonnable de vie privée, à ce moment-là l'employeur devra respecter un certain nombre de conditions dans le cadre l'exercice de la surveillance[254].

Les principaux facteurs applicables dans la détermination de l'expectative raisonnable de vie privée d'un employé qui utilise Internet au travail sont : i) la connaissance de la surveillance; ii) l'existence d'un consentement à l'égard de la surveillance; ii) la nature vulnérable des communications surveillées; iii) l'environnement de travail; et (iv) la nature personnelle des informations ou des renseignements recueillis. Nous allons passer en revue chacun de ces facteurs afin d'évaluer l'impact qu'ils peuvent avoir dans la détermination de l'expectative de vie privée d'un employé qui utilise Internet au travail.

---

[253] *Infra*, p. 115.

[254] *Infra*, p. 153.

2.2.1.2.2.1. *La connaissance de la surveillance*

Depuis quelques années, la pratique qui s'est développée au sein des entreprises consiste à adopter une politique d'utilisation d'Internet, informant l'employé de l'existence d'une surveillance, et de lui communiquer cette politique au moment de son embauche ou durant sa période d'emploi[255]. En effet, la croyance populaire est à l'effet qu'un employeur a le droit d'exercer une surveillance de l'utilisation d'Internet dès qu'il transmet une politique à cet effet à ses employés[256].

Il est reconnu que l'adoption d'une telle politique et sa mise à la connaissance au niveau des employés a pour effet de réduire l'expectative raisonnable de vie privée des employés[257]. Ce principe est d'ailleurs affirmé par l'auteur Marc-Alexandre Poirier[258] :

> « If employees are advised of the circumstances in which their e-mails may be intercepted, their reasonable expectation of privacy will be significantly diminished, if not completely negated. Obviously, no one can reasonably expect their communications to remain private if it is known in advance that they will be monitored. »[259]

Toutefois, malgré la croyance populaire, il faut bien comprendre qu'il s'agit là d'une réduction et non d'une disparition de l'expectative raisonnable de vie privée, tel qu'il

---

[255] A. LEVIN, M. FOSTER, M. J. NICHOLSON et T. HERNANDEZ, préc., note 142, p. 18; Colin H.H. MCNAIRN et Alexander K. SCOTT, *Privacy Law in Canada*, Markham (Ont.), Butterworths, 2001, p. 179 et 180; R. PERREAULT, préc., note 111, à la page 74.

[256] Cette croyance est d'ailleurs compatible avec l'approche récemment développée aux États-Unis quant à l'expectative raisonnable de vie privée à l'égard des courriels en général. Cette approche, notamment illustrée dans *United States* v. *Warshak*, 490 F.3d 455 (6th Cir. 2007), inf. par No. 06-4092, 2008 WL 2698177, 2008 U.S. App. LEXIS 14717 (6th Cir. July 11, 2008), affirme que si le fournisseur de services Internet a communiqué à l'utilisateur des services Internet une politique indiquant l'existence d'une surveillance, l'utilisateur ne peut raisonnablement s'attendre à ce que ses communications sur le réseau demeurent privée. Toutefois, en l'absence d'une telle politique, l'utilisateur peut, dépendamment des autres circonstances en l'espèce, disposer d'une attente raisonnable de vie privée à l'égard de ses courriels.

[257] *Blais et La Société des Loteries Vidéos du Québec Inc.*, préc., note 136, par. 95 et 96; et *United States* v. *Munroe*, 52 M.J. 326 (C.A.A.F. 2000). Dans la doctrine, voir : K. DELWAIDE, « L'Internet en milieu de travail et les politiques et directives relatives à l'utilisation des nouvelles technologies », préc., note 53, p. 33.

[258] M.-A. POIRIER, préc., note 143.

[259] *Id.*, 102.

ressort des propos de l'auteur Diane Veilleux[260] :

> « En effet, ce n'est pas parce que l'employeur informe les personnes salariées qu'il entend restreindre ou porter atteinte à leur droit à la vie privée que ce droit n'existe plus. L'attente raisonnable de vie privée s'évalue non pas en fonction de la connaissance du contrôle exercé, mais de la nature de celui-ci. »[261]

Il serait d'ailleurs illogique que l'existence d'un droit à la vie privée dépende de la volonté de celui qui veut la restreindre, tel que souligné par l'auteur Levin[262] :

> « The determination of whether workplace surveillance is reasonable is achieved independently of the employer's policies and notifications issued to workers, which seems to be the aspects most employers focus when attempting to legitimize their practices. »[263]

À cet égard, les propos du juge Laforest dans l'arrêt *R.* c. *Wong*[264], bien qu'énoncés en matière de surveillance par caméra vidéo dans une chambre d'hôtel, sont tout aussi pertinents dans le contexte de la surveillance de l'utilisation d'Internet : « La vie privée serait mal protégée si le caractère raisonnable de notre attente en matière de respect de la vie privée dépendait de la question de savoir si nous sommes exposés à la surveillance électronique. »[265]

L'existence de politiques de surveillance est l'un des facteurs qui a été considéré dans l'affaire *Blais* c. *La Société des loteries vidéos du Québec*[266] dans le cadre de l'analyse de l'expectative raisonnable de vie privée de l'employé dans l'utilisation d'Internet au travail. En l'espèce, l'employé savait que son employeur avait accès au contenu de son ordinateur, interceptait les communications électroniques, contrôlait la connexion Internet et pouvait conserver, archiver et utiliser les messages

---

[260] D. VEILLEUX, préc., note 241.

[261] *Id.*, 28.

[262] A. LEVIN, M. FOSTER, M. J. NICHOLSON et T. HERNANDEZ, préc., note 142.

[263] *Id.*, p. 9.

[264] Préc., note 178.

[265] *Id.*, par. 45.

[266] Préc., note 136.

électroniques et pièces jointes transigeant dans sa boîte de courriel. Non seulement plusieurs politiques avaient circulé à cet égard, mais l'employé avait reçu plusieurs avertissements et rappels de la part de son employeur.

Compte tenu de ces circonstances, la Commission a conclu qu'en aucun moment l'employé Blais n'avait disposé d'une expectative raisonnable de vie privée dans le cadre de son utilisation d'Internet. La connaissance que l'employé avait de l'exercice de la surveillance et du contrôle exercé par l'employeur à l'égard de l'utilisation d'Internet n'est toutefois pas le seul facteur considéré dans la décision, ce qui porte à croire que la seule existence des politiques de l'employeur n'aurait pu mener la Commission à la même conclusion. D'autres éléments sont également entrés en ligne de compte, notamment la propriété de l'employeur sur les biens surveillés. C'est donc l'ensemble des circonstances qui a fait en sorte que l'expectative raisonnable de vie privée était inexistante.

Plutôt que d'être vues comme un moyen permettant d'exercer légalement la surveillance, les politiques devraient plutôt être considérées comme des outils stratégiques au niveau de la gestion des risques liés à l'utilisation d'Internet. En effet, non seulement l'existence d'une politique permet de réduire l'expectative de vie privée de l'employé, mais elle aide l'employeur à s'acquitter de son fardeau de preuve en cas de sanction disciplinaire[267].

D'ailleurs, il nous apparaît important de souligner que l'absence de politique ou de

---

[267] Pour des illustrations jurisprudentielles ayant considéré l'existence d'une politique dans le cadre de l'analyse de la mesure disciplinaire prise à l'endroit d'un employé, voir : *Syndicat canadien des communications, de l'énergie et du papier, section locale 522 et C.A.E. Électronique ltée,* préc., note 95; *Syndicat de professionnelles et professionnels du gouvernement du Québec et Québec (Ministère du Revenu),* préc., note 136; *Blais et La Société des Loteries Vidéos du Québec Inc.,* préc., note 136; *Syndicat canadien de la fonction publique, section locale 4140 et Centres jeunesse de l'Outaouais*, préc., note 97; *Syndicat des spécialistes et professionnels d'Hydro-Québec, section locale 4250 (SCFP-FTQ) et Hydro-Québec*, préc., note 96; *Syndicat de la fonction publique du Québec – Fonctionnaires et Québec (Ministère de l'Emploi et de la Solidarité sociale)*, préc., note 97; et *Syndicat du personnel de soutien de la Seigneurie des Mille-Îles (CSN) et Commission scolaire de la Seigneurie-des-Mille-Îles*, préc., note 136. Pour des illustrations de mesures disciplinaires prises en l'absence de politique, voir : *Commission des normes du travail* c. *Bourse de Montréal*, préc., note 136; *Fiset* c. *Service d'administration P.C.R. Ltée*, (2003) R.J.D.T. 361 (C.T.); et *Belisle et Rawdon (Municipalité de)*, préc., note 136.

consentement de la part de la personne concernée n'entraîne pas nécessairement un empêchement à ce que l'employeur surveille l'utilisation d'Internet et sanctionne un comportement déviant[268]. Tel que nous le verrons au prochain chapitre, les obligations d'information et de consentement sont sujettes à certaines exceptions[269].

Par ailleurs, l'existence de politiques écrites n'est pas le seul pour un employeur d'établir la connaissance de la surveillance par les employés et dès lors la baisse de leur expectative de vie privée à l'égard des activités surveillées. En effet, par analogie avec les principes établies en matière de fouille au travail[270], nous pouvons affirmer que si la surveillance de l'utilisation d'Internet constitue une pratique habituelle ou établie au sein de l'entreprise qui fait implicitement partie des conditions de travail de employés, l'employeur est alors en mesure de démontrer que les employés connaissent cette politique et les circonstances dans lesquelles elle est appliquée. Tel qu'indiqué par la doctrine en matière de fouille, « [l]a pratique de surveillance fait alors partie des conditions de travail au même titre que si elle apparaissait dans le livre des règlements de l'employeur ou dans la convention collective. »[271]

Pour pouvoir parler de pratique établie constituant une condition d'emploi, l'employeur doit avoir appliqué la politique de surveillance de manière suffisamment fréquente et universelle auprès de ses employés depuis plusieurs années, et ce sans avoir agit de manière discriminatoire[272].

2.2.1.2.2.2. *Le consentement à la surveillance*

---

[268] R. PERREAULT, préc., note 111, à la page 85.

[269] *Infra*, p. 166.

[270] Linda BERNIER, Lukasz GRANOSIK et Jean-François PEDNEAULT, *Les droits de la personne et les relations du travail*, Cowansville, Éditions Yvon Blais, 1997, feuilles mobiles, à jour au 10 décembre 2008 (n° 23, Nov. 2008), par. 21.072.

[271] *Id.*

[272] *Id.*, par. 21.073 et 21.074. Pour des illustrations jurisprudentielles de ce principe en matière de fouille, voir : *Syndicat international des travailleurs de la boulangerie, confiserie et du tabac, section locale 476 F.A.T.-C.I.O.-C.T.C. et Walter M. Lowney Co.*, [1983] T.A. 665, D.T.E. 83T-423; *Syndicat des travailleurs de l'énergie et de la chimie, section locale 107* c. *Laurin*, D.T.E. 91T-841, AZ-91029087 (C.S.); et *Corp. Outils Québec et Syndicat indépendant des salariés de Outils Québec*, [1992] T.A. 646, D.T.E. 92T-933.

Par ailleurs, qu'arrive-t-il quand un employé signe au bas de la politique distribuée par l'employeur à l'effet qu'il consent à ce que l'employeur exerce une surveillance de l'utilisation d'Internet suivant les termes et conditions énoncés dans la politique? Est-ce que son droit à la vie privée disparaît?

Nous pourrions croire qu'un employé qui consent explicitement ou implicitement à la surveillance renonce, par le fait même, au respect de son droit à la vie privée, et qu'une telle renonciation permettrait à l'employeur de surveiller l'utilisation d'Internet au travail. L'article 35 C.c.Q. prévoit en effet la possibilité pour l'employé de renoncer au respect de son droit à la vie privée. Le cas échéant, l'employé ne disposerait d'aucune expectative de vie privée et l'employeur n'aurait pas à se soucier de remplir les conditions applicables aux restrictions au droit à la vie privée des employés[273].

Toutefois, au Québec, pour être valide, la renonciation à un droit fondamental doit être claire, non équivoque et volontaire[274]. Dans le contexte d'une relation de travail, il apparaît difficile de conclure au caractère volontaire d'une signature apposée par un employé sur une politique émanant de son employeur, compte tenu que l'employé ne dispose normalement pas d'un pouvoir de négociation lors de l'émission du consentement et qu'une telle renonciation découle généralement d'un choix inéquitable[275].

Dans la majorité des cas, l'employé, subordonné à son employeur, est placé dans une situation où il est, à toutes fins utiles, obligé de se soumettre à la surveillance de

---

[273] M.-A. POIRIER, préc., note 143, 103; et D. VEILLEUX, préc., note 241, 35 : « La renonciation au respect de sa vie privée enlève à la personne salariée le droit d'exiger que l'employeur démontre la rationalité et la proportionnalité de la restriction imposée à ce droit par la surveillance exercée. »

[274] *R.* c. *Morin*, [1992] 1 R.C.S. 771, 790; *Syndicat des employées et employés professionnels et de bureau, section locale 57 et Caisse populaire St-Stanislas de Montréal*, préc., note 241, 362 et 363; et Maxime LAMOTHE, *La renonciation à l'exercice des droits et libertés garantis par les chartes*, Cowansville, Les Éditions Yvon Blais, 2007, p. 173 et suiv.

[275] Pour une analyse du caractère volontaire de la renonciation en milieu de travail, voir D. VEILLEUX, préc., note 241, 31-35.

l'employeur, au risque de ne pas être engagé, d'être confronté à l'employeur, ou encore être congédié. Dans ce contexte, le consentement de l'employé ne peut être donné de façon volontaire et équivaut à l'acceptation d'un contrat d'adhésion[276].

Bien que la Cour suprême du Canada ait déjà confirmé la possibilité d'une renonciation à la vie privée par voie contractuelle dans l'arrêt *Frenette c. Métropolitaines (La), cie d'assurance-vie*[277], cet arrêt ne portait pas sur la validité de la renonciation ni sur son caractère volontaire. De plus, il s'agissait en l'espèce d'un contrat d'assurance-vie plutôt que d'un contrat de travail. Dans ce contexte, la possibilité d'une renonciation à la confidentialité semblait inévitable. Par conséquent, les principes énoncés dans cet arrêt ne sont pas applicables dans le contexte d'un consentement à l'exercice d'une surveillance au travail[278].

La Cour suprême du Canada a d'ailleurs confirmé cette position dans l'arrêt *Godbout c. Ville de Longueuil*[279]. En l'espèce, l'employée avait été soumise à deux choix : soit elle quittait son poste, soit elle accédait à la permanence en s'engageant à demeurer à Longueuil pendant toute la durée de son emploi. La Cour a clairement affirmé que les principes énoncés dans l'arrêt *Frenette* c. *Métropolitaines (La), cie d'assurance-vie*[280] n'étaient pas applicables dans ce contexte[281] et a conclu que l'acquiescement exprimé par la signature de l'employé ne pouvait équivaloir à une renonciation à son droit protégé par l'article 7 de la Charte canadienne. La Cour s'est exprimée dans les termes suivants :

> « Tout simplement, l'intimée n'a pas eu la possibilité de négocier la clause

---

[276] Le contrat d'adhésion est défini à l'article 1379 C.c.Q. de la manière suivante : « Le contrat est d'adhésion lorsque les stipulations essentielles qu'il comporte ont été imposées par l'une des parties ou rédigées par elle, pour son compte ou suivant ses instructions, et qu'elles ne pouvaient être librement discutées. »

[277] [1992] 1 R.C.S. 647.

[278] D. VEILLEUX, préc., note 241, 32; *contra* : *Regroupement des travailleuses et travailleurs du Québec et Sécur (division guichets automatiques)*, [2002] R.J.D.T. 846 (T.A.).

[279] *Godbout* c. *Ville de Longueuil*, préc., note 174.

[280] Préc., note 278.

[281] *Godbout* c. *Ville de Longueuil*, préc., note 174, par. 93.

> obligatoire de résidence et, par conséquent, on ne peut à toutes fins utiles considérer qu'elle a renoncé librement à son droit de choisir le lieu où elle veut vivre. Pour parler en civiliste, l'acquiescement exprimé par la signature de la déclaration de résidence équivalait pratiquement à l'acceptation d'un contrat d'adhésion (...) et ne peut ainsi être valablement interprété comme une renonciation. »[282]

Pour que l'on puisse conclure au caractère volontaire d'une renonciation d'un employé dans le contexte d'une relation de travail avec un employeur, il faudrait que l'employé ait la possibilité de négocier de gré à gré avec l'employeur quant à l'étendue de la surveillance de l'employeur. En principe, le consentement donné ne pourra équivaloir à une renonciation valide[283].

Cette position est d'ailleurs renforcée par le fait qu'en matière de protection des renseignements personnels, la loi impose, malgré l'existence d'un consentement de la part de la personne concernée, des conditions quant aux fins pour lesquelles une organisation recueille, détient ou communique des renseignements personnels. Tel que souligné par l'ancien commissaire fédéral à la vie privée George Radwanski[284] :

> « L'employeur peut faire du consentement à la collecte, à l'utilisation ou à la communication de renseignements personnels une condition d'embauche ou de maintien en poste, tant et si bien que le consentement peut devenir une simple formalité. C'est la raison pour laquelle le critère de la personne raisonnable sur lequel est fondée l'application de la *LPRPDÉ* devient si important. »[285]

Par ailleurs, qu'en est-il si la convention collective de l'entreprise contient une clause en vertu de laquelle les employés renoncent à leur droit à la vie privée dans l'utilisation d'Internet, par exemple en prévoyant expressément qu'une surveillance

---

[282] *Id.*, par 72.

[283] *Syndicat des professionnelles du Centre jeunesse de Québec (CSN)* c. *Desnoyers,* [2005] R.J.Q. 414, 422, inf. par 2008 QCCA 1911; et *Syndicat des employées et employés professionnels et de bureau, section locale 57 et Caisse populaire St-Stanislas de Montréal*, préc., note 241, 363 (à l'effet que les cas de renonciation doivent être interprétés restrictivement, particulièrement s'il s'agit d'une renonciation implicite).

[284] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Conférence sur la vie privée au travail*, discours de George Radwanski, Vancouver, 23 mai 2003, en ligne : http://www.privcom.gc.ca/speech/2003/02_05_a_030529_f.asp.

[285] *Id.*, p. 5. Voir également *X.* c. *Laval (Société de transport de la Ville de)*, [2001] C.A.I. 226 (C.A.I.), 238 : « Tout consentement d'un individu, en matière de renseignement personnel le concernant, ne peut s'étendre au-delà de ce que la loi autorise cet organisme à cueillir, conserver ou communiquer. », conf. par *Laval (Société de transport de la Ville de)* c. *X.*, [2003] C.A.I. 667 (C.Q.), 671.

de l'utilisation d'Internet sera mise en place à l'égard de tous les employés de l'entreprise; est-ce que l'on peut considérer qu'il s'agit d'une renonciation négociée librement par les parties?

À première vue, il semblerait que la réponse est positive, compte tenu que le consentement du syndicat peut équivaloir au consentement des employés[286]. En effet, les conventions collectives sont généralement des instruments négociés librement par des parties ayant un pouvoir relativement égal et faisaient exception à la règle voulant qu'on ne puisse renoncer par contrat à l'application d'une loi sur les droits de la personne[287].

Toutefois, compte tenu de la difficulté d'obtenir une égalité parfaite même dans le contexte d'une convention collective, il peut être difficile pour un tribunal d'affirmer que la renonciation obtenue a fait disparaître toute expectative raisonnable de vie privée de l'employé, et permet à l'employeur de surveiller l'utilisation d'Internet par les employés.

Par conséquent, bien que pouvant constituer une renonciation valide à un droit fondamental, une telle clause demeurera soumise aux critères applicables pour porter atteinte aux droits fondamentaux, et ce afin de s'assurer que la restriction en question est justifiée par des intérêts légitimes et suffisamment importants. Tel que souligné par la Cour suprême dans l'arrêt *Dickason* c. *Université de l'Alberta*[288], les conventions collectives ne sont pas dépourvues de dangers et il arrive parfois qu'un syndicat choisisse de négocier une clause qui profite uniquement à la majorité des membres, aux dépens des intérêts de la minorité[289]. Il faut donc être conscient de cette possibilité lorsque l'on analyse l'impact d'une clause contenue dans une convention

---

[286] *Association internationale des machinistes et des travailleuses et travailleurs de l'aérospatiale, section locale 2468 et Rolls-Royce Canada ltée*, D.T.E. 2001T-153 (T.A.).

[287] *Dickason* c. *Université de l'Alberta,* [1992] 2 R.C.S. 1103, 1130 et 1131.

[288] *Id.*

[289] *Id.*, 1131.

collective à l'égard du respect des droits fondamentaux des employés.

Par conséquent, au même titre qu'une renonciation individuelle, une renonciation obtenue par le biais d'une convention collective ne pourra automatiquement faire disparaître toute expectative raisonnable de vie privée des employés, et ne pourra jamais avoir pour effet de soustraire un employeur de l'application des critères découlant des articles 9.1 de la Charte québécoise, de l'article 1 de la Charte canadienne ou encore du critère de nécessité prévu dans les lois sur la protection des renseignements personnels[290]. Dans tous les cas, une renonciation valide à un droit fondamental obtenue par le biais d'une convention collective ne constituera qu'un facteur applicable dans l'appréciation de l'attente raisonnable de vie privée de l'employé, ayant pour effet de réduire ce niveau d'expectative.

2.2.1.2.2.3. *La nature vulnérable des communications Internet*

Tel que mentionné précédemment, la vie privée est une notion qui évolue constamment dans le temps et dans l'espace. À cet effet, l'évolution et l'apparition constante de nouvelles technologies contribuent constamment à faire évoluer le sens de cette notion. En 1890, les auteurs Warren et Brandeis soulignaient déjà, dans un article qui est devenu l'une des références clés au sujet de la notion de vie privée[291], les risques causés par les nouvelles technologies sur la protection de la vie privée :

> « Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that « what is whispered in the closet shall be proclaimed from the house-tops. »[292]

---

[290] *Infra*, p. 128. Voir : *Syndicat canadien des communications, de l'énergie et du papier, section locale 233 et Tembec inc.*, [2000] R.J.D.T. 1285, D.T.E. 2000T-855 (T.A.) à l'égard d'une clause contenue dans une convention collective obligeant les employés d'une entreprise à demeurer dans une rayon de 15 milles des usines situées à Témiscaminque. Invoquant l'arrêt *Dickason*, l'arbitre André Sylvestre a conclu que la clause en question était valide et constituait une renonciation à un droit garanti par la Charte québécoise, compte tenu notamment qu'elle avait été négociée librement par le syndicat et qu'elle passait le test de l'article 9.1 de la Charte québécoise.

[291] S. D. WARREN et L. D. BRANDEIS, préc., note 224.

[292] *Id.*, 195.

Plus d'un demi-siècle plus tard, le même principe a été reformulé par le président américain Lyndon B. Johnson :

> « The principle that a man's home is his castle is under new attack. For centuries the law of trespass protected a man's lands and his home. But in the age of advanced technology, thick walls and locked doors cannot guard our privacy or safeguard our personal freedom. »[293]

Certaines particularités propres aux communications Internet ont pour effet de réduire le niveau d'expectative de vie privée des utilisateurs par rapport aux communications effectuées par voies traditionnelles[294]. Dans ce contexte, la détermination de l'expectative raisonnable de vie privée exige la prise en compte de ces particularités, tant au niveau de l'utilisation du courrier électronique que de la messagerie instantanée.

Jusqu'à aujourd'hui, peu de tribunaux se sont penchés sur cette question. Bien qu'il soit possible d'affirmer que le contenu d'un ordinateur de même que le contenu d'une boîte de courrier électronique peut relever du domaine de la vie privée[295], les tribunaux québécois qui ont analysé le niveau d'expectative de vie privée dans le cadre de l'utilisation d'Internet n'ont pas considéré les particularités propres aux communications Internet ou à la navigation sur le Web dans le cadre de leur analyse[296]. Sur cette question, nous devons nous référer à l'arrêt *R.* v. *Weir*[297] rendu

---

[293] Propos cités dans André BACARD, *The Computer Privacy Handbook*, Berkeley (Calif.), Peachpit Press, 1995, p. 21.

[294] Pour une analyse détaillée de l'expectative raisonnable de vie privée dans les principaux contextes de communications sur Internet, voir F. BLANCHETTE, préc., note 236. Pour des illustrations jurisprudentielles de la reconnaissance de l'expectative de vie privée à l'égard du courrier électronique, voir : *R.* v. *Weir*, préc., note 182. Aux États-Unis, voir *United States* v. *Maxwell*, 42 M.J. 568 (A.F.C.C.A. 1995), inf. en partie par 45 M.J. 406, 1997 WL 643294 (A.F.C.C.A. 1997); *United States* v. *Charbonneau*, 979 F. Supp. 1177 (S.D. Ohio 1997), p. 1184; *Commonwealth of Pennsylvania* v. *Proetto*, 2001 Pa. Super 95, 771 A.2d 823, 92 A.L.R.5th 681 (2001), inf. en partie par 567 Pa. 667, 790 A.2d 988 (2002); *United States* v. *Warshak*, préc., note 256; et *United States* v. *Ziegler*, préc., note 163.

[295] *R.* c. *Tremblay*, préc., note 159; *R.* c. *Gauthier*, préc., note 183; *Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada*, préc., note 136; *Blais et La Société des Loteries Vidéos du Québec Inc.*, préc., note 136; *R.* v. *Weir*, préc., note 182; et *U.S.* v. *Maxwell,* préc., note 294.

[296] *Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada*, préc., note 136; *Blais et La Société des Loteries Vidéos du Québec Inc.*, préc., note 136; et *Syndicat des professionnelles et professionnels des affaires sociales du Québec (C.S.N.) et Institut de réadaptation en déficience physique de Québec*, préc., note 154.

en Alberta de même qu'à certains arrêts américains dont les principes devraient être repris au Québec. Voyons comment ces différentes particularités entrent en ligne de compte dans l'analyse de l'expectative raisonnable de vie privée.

2.2.1.2.2.3.1 Comparaison avec les communications traditionnelles

Afin d'évaluer l'impact des nouvelles technologies sur l'expectative raisonnable de vie privée des personnes qui l'utilisent, il convient en premier lieu de comparer les communications Internet aux communications par voies traditionnelles, telles que le courrier postal et le téléphone.

À cet égard, la question à savoir si nous devons assimiler l'expectative de vie privée à l'égard des communications faites par le biais d'Internet à celle relative aux médiums de communications traditionnels demeure très controversée. Certains comparent les communications Internet avec les conversations téléphoniques ou le courrier postal[298], ou comparent la surveillance de l'utilisation d'Internet aux fouilles physiques ou à la surveillance par caméra vidéo. D'autres affirment qu'il y a réellement des distinctions à faire, que ce soit avec le courrier postal ou avec les conversations téléphoniques, compte tenu de la nature très particulière des communications faites par le biais d'Internet.

En France les tribunaux assimilent généralement le courrier électronique au courrier postal, lequel est protégé par la *Loi no. 91-646 du 10 juillet 1991 relative au secret des correspondances par voie de télécommunication*[299]. Dans l'arrêt *Société Nikon France SA c/ M. Onof*[300], la Cour de Cassation a d'ailleurs affirmé que la surveillance

---

[297] Préc., note 182. Bien que cet arrêt ait été porté en appel, la Cour d'appel d'Alberta n'a pas traité de la question de l'expectative raisonnable de vie privée dans son jugement. Par conséquent, nous devons nous en remettre à la décision du juge Smith sur cette question.

[298] Voir notamment *United States* v. *Warshak*, (6th Cir. July 11, 2008), préc., note 256, p. 9-15.

[299] JO n° 162 du 13 Juillet 1991, p. 9167 et 10 août 1991 (rectificatif), p. 10617.

[300] Soc. 2 octobre 2001, *Bull. civ.* V, no. 291.

du courrier électronique personnel d'un employé violait le secret des correspondances[301]. Par la suite, en 2004, la loi française relative au secret des correspondances a été modifiée afin d'inclure les communications électroniques[302]. Les courriels doivent donc recevoir la même protection que le courrier postal.

Au Québec, contrairement à la position adoptée en France, les tribunaux semblent plutôt portés à comparer l'usage d'Internet avec le téléphone et à s'inspirer des principes applicables en la matière pour analyser la légalité de la surveillance[303]. Cette tendance s'est toutefois développée dans le cadre de l'appréciation de la faute d'un employé suite à un usage abusif d'Internet à des fins personnelles. Bien qu'il soit possible de s'inspirer de ces principes, ceux-ci doivent être appliqués avec réserve dans le cadre de l'analyse de l'expectative de vie privée de l'utilisateur. En effet, bien qu'un employé puisse utiliser Internet à des fins personnelles au même titre que le téléphone, cela ne signifie pas que son expectative de vie privée à l'égard des deux moyens de communications soit la même.

Par ailleurs, dans l'arrêt *R.* v. *Weir*[304], le juge Smith fait un parallèle entre les différents moyens de communication, en soulignant notamment les similitudes entre le courrier électronique et le courrier postal :

> « They both support powerful one to one communications, encourage users to express their thoughts to others in print, feature private mailboxes controlled by the person receiving the mail, support delivery of written documents in a timely manner directly to the addressee, allow for large amounts of additional material to be included, can be

---

[301] *Id.*, p. 1 : « Attendu que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur. »

[302] Modifié par *Loi n°2004-669 du 9 juillet 2004,* art. 125 (JORF 10 juillet 2004). Le titre de la loi est maintenant *Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.*

[303] *Syndicat canadien des communications, de l'énergie et du papier, section locale 522 et C.A.E. Électronique ltée,* préc., note 95, p. 334; et *Bell Canada et Association canadienne des employés de téléphone*, préc., note 136, 365.

[304] Préc., note 182.

> easily copied and sent to others or saved indefinitely, involve a delay between transmission and reception as well as between reception of the message and any response, support the communication of a message by the sender uninterrupted by the recipient, enhance communication between people who have never met, are relatively cheap and the cost of domestic transfer is not usually affected by the location of the recipient, allow a recipient to know either who a communication is from or where it originated before reading it, wait for the recipient and can be read on the recipient's own time, once sent cannot be retrieved, make bulk mailings and junk mail easy to send to unwanting recipients, with neither can a sender know immediately if a message has received its intended destination, both are sent out in batches, and, last, both can be subject to fraudulent use. »[305]

Dans son jugement, le juge Smith souligne également les similitudes entre le courrier électronique et le téléphone :

> « The primary similarity between the two is technology. Both e-mail and telephone calls travel over the same wires and require little effort on the part of the sender. Both can be transmitted essentially with the stroke of a few keys. There is no need to leave the house. Both may be received more than once a day. Neither requires manpower for delivery. Technology and an infrastructure is required to use both. Without it, messages can neither be sent or received. And last, e-mail can be used for the same type of simultaneous discussion that telephone communications are intended to be. »[306]

Finalement, il mentionne les caractéristiques propres au courrier électronique :

> « It is one of the most cost efficient forms of communication available. E-mail address systems allow for anonymity if desired by the sender. The address system allows for automatic reply with little effort. Also, Netiquette, a body of generally accepted rules of behavior, has been developed for e-mail and Internet communications in general. For example, uppercase letters signify the sender is yelling. Netiquette behaviors imply that replying to e-mail messages is easier than replying to other communications. »[307]

À la lumière de cette analyse, il conclut que l'expectative raisonnable de vie privée à l'égard du courrier électronique est moindre qu'à l'égard du courrier postal :

> « These facts about the technology help me to conclude the e-mail message is unlike first class mail in the level of privacy that it can attract. (...) In summary, I am satisfied e-mail via the Internet ought to carry a reasonable expectation of privacy.

---

[305] *Id.*, par. 62.

[306] *Id.*, par. 63.

[307] *Id.*, par. 64.

> Because of the manner in which the technology is managed and repaired that degree of privacy is less than that of first class mail. Yet the vulnerability of e-mail requires legal procedures which will minimize invasion. »[308]

Il ressort de l'arrêt *R.* v. *Weir*[309] les constats suivants : (i) bien que nous puissions nous inspirer des principes applicables en matière d'écoute téléphonique, de surveillance vidéo ou de secret des correspondances, il ne suffit pas simplement de nous y référer par analogie pour déterminer le niveau d'expectative raisonnable de vie privée dans l'utilisation d'Internet; (ii) les communications faites par le biais d'Internet comportent des particularités qui leurs sont propres et qui imposent de nouveaux facteurs lors de l'analyse de l'expectative raisonnable de vie privée; et (iii) ces particularités propres aux communications Internet sont les suivantes : (1) la mise en évidence des entêtes et pièces jointes au message; (2) la possible interception des communications Internet; (3) la perte de contrôle de l'expéditeur une fois le message transmis; et (4) les traces laissées par les activités Internet dans l'ordinateur de l'utilisateur.

Par ailleurs, nous tenons à souligner que la plupart des particularités liées à Internet se rattachent uniquement aux communications Internet et n'affectent pas l'expectative de vie privée d'un utilisateur dans le cadre des autres types d'activités menés sur Internet, tels que la navigation sur le Web ou les blogs. Ainsi, presque toutes les particularités qui seront ci-après exposées ne s'appliquent qu'à l'utilisation du courrier électronique, de la messagerie instantanée, ou de tout autre système permettant de communiquer par Internet. Seules les traces laissées dans l'ordinateur de l'utilisateur affectent l'ensemble des activités Internet et ont un impact sur l'expectative de vie privée pour toutes ces activités. En effet, tant les communications Internet, la participation à des forums de discussion, la navigation sur le web que la création de pages ou de sites web, laissent des traces dans l'ordinateur de l'utilisateur.

---

[308] *Id.*, par. 74 à 77.

[309] *Id.*

2.2.1.2.2.3.2 Les entêtes, les pièces jointes et le corps du message

Un message par courrier électronique comporte différentes parties : i) le corps du message, dans lequel l'expéditeur rédige son message; et ii) les champs d'en-tête, qui décrivent les paramètres du message, tels que l'expéditeur, le destinataire, la date et l'objet du message. Un courriel peut également être accompagné de différents fichiers de différents formats et de différents volumes. Toutes les informations mentionnées dans les champs d'en-tête et au niveau des pièces jointes sont généralement mises en évidence dans la boîte de courrier électronique, et ce sans même avoir à ouvrir le message.

À cet égard, le juge Smith, dans l'arrêt *R. c. Weir*[310], compare l'enveloppe du courrier postal aux champs d'en-tête d'un courriel. Selon lui, les informations contenues dans les champs d'en-tête font l'objet d'une expectative de vie privée moindre que celle relative au corps du message, au même titre que l'expectative de vie privée à l'égard des informations se retrouvant sur l'enveloppe d'une lettre postale (adresses du destinataire et du destinateur, date) est moindre que celle relative au contenu de la lettre.

Le même principe s'applique à l'égard des pièces jointes à un message transmis par courrier électronique. En effet, lorsque l'on a accès aux champs d'en-tête, on a généralement accès à la liste des pièces jointes au message, au nom des fichiers de même que leur volume respectif. L'expectative de vie privée de l'employé à l'égard de ces informations est donc moindre que celle relative au contenu du message.

Quant à l'expectative de vie privée de l'employé à l'égard du corps du message, soit le contenu du message, celle-ci sera plus élevée que celle relative aux informations contenues dans les champs d'entêtes ou les noms des fichiers joints, compte tenu

---

[310] *Id.*

qu'un employé pourra généralement s'attendre à ce que l'employeur n'aille pas jusqu'à ouvrir ses courriels et lire leur contenu[311].

C'est d'ailleurs dans cette optique que la Cour d'appel du 6e district fait un parallèle avec le courrier postal dans l'arrêt *United States* v. *Warshak*[312] pour affirmer que l'utilisateur qui transmet un courriel peut raisonnablement s'attendre à ce que le contenu de ses courriels enregistrés sur le réseau demeure privé, et ce dans les termes suivants : « In fact, these screening processes are analogous to the post office screening packages for evidence of drugs or explosives, which does not expose the content of written document enclosed in the package. »[313]

2.2.1.2.2.3.3. L'interception des communications Internet

Une autre particularité propre aux communications Internet et qui pourrait être soulevée dans le cadre de l'analyse de l'expectative de vie privée est la facilité avec laquelle il est possible d'intercepter les messages. En effet, les communications Internet peuvent être facilement interceptées[314] et certains affirment que le niveau de sécurité d'un courrier électronique en transit est le même que celui d'une carte postale[315], à moins bien sûr que le message ne soit chiffré.

---

[311] Par analogie avec les propos énoncés dans la décision *United States* v. *Warshak*, (6th Cir. 2007), préc., note 256, p. 11 : « The combined precedents of Katz and Smith, however, recognize a heightened protection for the content of the communications. Like telephone conversations, simply because the phone company or the ISP could access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do as a matter of course. »

[312] *Id.*

[313] *Id.*, p. 13. Dans la doctrine, voir : William A. HEBERT, « The Electronic Workplace : To Live Outside the Law You Must Be Honest », (2008) 12 *Employee Rts. & Emp. Pol'y J.* 49.

[314] M.-A. POIRIER, préc., note 143, 91 : « The protocol used to effect Internet transmissions is such that the messages can easily be accessed or viewed by intermediary computers unless encrypted ». Voir également F. BLANCHETTE, préc., note 236, p. 114; et René PÉPIN, « Le statut juridique du courriel au Canada et aux États-Unis », (2001) 6-2 *Lex electronica*, en ligne : http://www.lex-electronica.org/articles/v6-2/pepin.htm, p. 4.

[315] M.-A. POIRIER, préc., note 143, 90; et F. BLANCHETTE, préc., note 236, p. 115.

Nous ne faisons pas ici référence à l'interception des communications par l'employeur au moyen d'une surveillance. Nous faisons référence à une tierce personne qui intercepterait une communication Internet à l'insu des personnes concernées. Compte tenu qu'il est techniquement facile d'intercepter les communications Internet d'une personne à son insu, certains pourraient être tentés d'affirmer que cela réduit l'expectative de vie privée que cette personne peut avoir face à ces communications.

Cette affirmation est toutefois erronée. La question qu'il faut se poser n'est pas à savoir s'il est techniquement possible d'intercepter le message, mais plutôt si la personne concernée pouvait raisonnablement s'attendre à ce que son message soit réellement intercepté. En effet, tout dépend plutôt de la méthode de transmission du message, compte tenu que les risques réels (et non la possibilité technique) d'interceptions des messages en transit varient selon le système et le contexte de transmission.

À cet effet, nous pouvons appliquer par analogie les principes énoncés par la Cour d'appel du Québec dans l'affaire *R.* c. *Solomon*[316]. En l'espèce, il s'agissait de l'interception des conversations téléphoniques tenues sur un téléphone cellulaire alors que la personne se trouvait à l'intérieur de sa voiture, portes et fenêtres fermées, et la Cour s'est exprimée comme suit :

> « J'estime que l'utilisateur d'un tel système est fondé à s'attendre et croire que ses conversations resteront privées même s'il n'ignore pas que des équipements, plus ou moins sophistiqués, peuvent permettre de capter ses paroles. (...) Les circonstances fixent l'attente de vie privée et l'existence de moyens technologiques propres à la violer ne la réduit et encore moins ne l'annule pas, à moins de nier le principe même de préservation de la vie privée. Ainsi, il y aura attente de confidentialité si des interlocuteurs prennent le soin de s'isoler dans un parc et de ne converser que s'ils sont seuls même si chacun sait qu'il est possible d'écouter ce qui se dit, à distance et sans être vu, grâce à un capteur semblable à ceux utilisés par les ornithologues pour enregistrer le chant des oiseaux alors qu'au contraire, l'attente sera inexistante si ces mêmes personnes

---

[316] Préc., note 181.

> se retrouvent dans un restaurant bondé. »[317]

D'ailleurs, en matière de courrier électronique, tel que souligné par Marc-Alexandre Poirier, les risques d'interceptions d'un message en transit sont extrêmement faibles, vu le nombre de courriels transigeant simultanément sur Internet :

> « First, the actual risk of any particular e-mail being intercepted is extremely remote. While e-mail messages may be technically easy to intercept, the sheer volume of e-mails circulating at any given time over the Internet significantly reduces the risk of interception (according to one report, at the end of 2000 there were 891.1 million electronic mailboxes in the world). Even a user who is tech-savvy enough to know that, while interception remains a possibility, in all probability the particular e-mail message he or she sends will not be viewed by anyone other than its intended recipient(s). »[318]

Par conséquent, le fait qu'il soit techniquement facile d'intercepter un message par courrier électronique n'a pas nécessairement pour effet de diminuer l'expectative de vie privée de l'expéditeur ou du destinataire. Dans le contexte d'une transmission d'un courrier électronique, ces derniers seront généralement en droit de s'attendre à ce que le message ne soit pas intercepté en cours de transmission, tel qu'il ressort des propos de la Cour d'appel des forces armées des États-Unis dans l' arrêt *U.S.* v. *Maxwell*[319] :

> « The sender enjoys a reasonable expectation that the initial transmission will not be intercepted by the police. The fact that an unauthorized "hacker" might intercept an e-mail message does not diminish the legitimate expectation of privacy in any way. » [320]

Dans cet arrêt américain, la Cour d'appel des forces armées américaines affirme par ailleurs que l'expectative de vie privée à l'égard d'une communication Internet dépend de la méthode de transmission[321]. Selon la Cour, les messages transmis par le

---

[317] *Id.*, 1795.

[318] M.-A. POIRIER, préc., note 143, 91.

[319] (A.F.C.C.A. 1997), préc., note 294.

[320] *Id.*, 418.

[321] *Id.*, p. 12 : « The more open the method of transmission, such as the « chat room », the less privacy one can reasonable expect. ». Voir également : *United States* v. *Charbonneau*, préc., note 295, 1184 (analyse de l'expectative de vie privée de l'utilisateur d'une chambre de chat); *Guest* v. *Leis*, 255 F.3d 325 (6th Cir. 2001), 333. (analyse de l'expectative de vie privée de l'utilisateur d'un forum de discussion Internet); et *Commonwealth of Pennsylvania* v. *Proetto*, préc., note 294, par. 27 (analyse de l'expectative de vie privée de l'utilisateur d'une chambre de chat).

biais du réseau d'AOL font l'objet d'une plus grande expectative raisonnable de vie privée compte tenu de la façon dont les messages sont centralisés et sécurisés. Quant aux messages transmis sur les réseaux ouverts tels que les chambres de *chat*, ceux-ci font l'objet d'une plus petite expectative de vie privée, compte tenu de la présence simultanée de tiers sur le réseau de communication. Le cas échéant, l'expéditeur du message ne peut s'attendre à ce que ses communications ne soient pas interceptées par les autres personnes présentes dans la même conversation, même si le message ne leur est pas destiné.

Par ailleurs, il est possible d'utiliser des techniques de cryptographie pour empêcher que des tiers auxquels le message n'est pas destiné prennent connaissance du contenu d'un message transmis par courrier électronique. Ces techniques comprennent notamment le chiffrement des messages, qui consiste à « substitue[r], à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale »[322]. Dans le cas où un message serait chiffré, l'expectative raisonnable de vie privée serait plus élevée, et même plus élevée que celle relative au courrier postal[323].

2.2.1.2.2.3.4. La perte de contrôle de l'expéditeur une fois le message transmis

La perte de contrôle de l'expéditeur, une fois qu'un message est transmis par le biais d'Internet, peut avoir pour effet de réduire l'expectative de vie privée de l'expéditeur, compte tenu que ce dernier ne peut prévoir ce que le destinataire fera du message[324].

Une fois reçu, le message peut être facilement copié ou retransmis à d'autres destinataires. À cet égard, nous pouvons tracer un parallèle avec le courrier postal une

---

[322] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE (OQLF), « Le grand dictionnaire terminologique », en ligne : http://www.granddictionnaire.com.

[323] F. BLANCHETTE, préc., note 236, p. 114.

[324] *Commonwealth of Pennsylvania* v. *Proetto*, préc., note 294, par. 21. Voir également *United States* v. *Charbonneau*, préc., note 294, 1184; et F. BLANCHETTE, préc., note 236, p. 124.

fois que l'enveloppe postale est ouverte :

> « E-mail transmissions are not unlike other forms of modern communications. We can draw parallels from these other mediums. For example, if a sender of first-class mail seals an envelope and addresses it to another person, the sender can reasonably expect the contents to remain private and free from the eyes of the police absent a search warrant founded upon probable cause. (...) However, once the letter is received and opened, the destiny of the letter then lies in the control of the recipient of the letter, not the sender, absent some legal privilege. »[325]

Dans ce contexte, certains affirment que les fonctions rattachées à la réponse d'un courriel ont pour effet de diminuer les attentes raisonnables de vie privée de l'expéditeur :

> « Les fonctions rattachées à la réponse à un courriel posent donc certains problèmes. En effet, les fonctions de réponse à l'auteur d'un message, de réponse à tous les destinataires d'un message, de redirection de message et de celles permettant de faire suivre un message, favorisent une diminution de l'expectative raisonnable de vie privée de l'expéditeur initial du message. Ces fonctions favorisent en quelque sorte la diffusion d'un courriel aux tiers : un expéditeur n'a pas de contrôle sur ce que le destinataire fera subséquemment du courriel envoyé et reçu. Conséquemment, dans la mesure où le courriel arrive à destination, l'expéditeur perd un certain degré d'expectative raisonnable de vie privée à son égard, tant au niveau du contenu que des informations techniques qui s'y rattachent. »[326]

Dans l'affaire *Briar* c. *Conseil du Trésor (Solliciteur général du Canada - Service correctionnel)*[327], la Commission des relations de travail du Canada a d'ailleurs considéré le fait que le salarié perdait contrôle de sa vie privée lorsqu'il cliquait sur le bouton « envoyer » de sa boîte des courriels au travail, pour conclure en l'absence d'expectative de vie privée à l'égard des courriels[328].

Toutefois, tel que mentionné précédemment, ce ne sont pas les particularités techniques permettant d'accéder aux communications Internet qui ont pour effet de

---

[325] *U.S.* v. *Maxwell,* (A.F.C.C.A. 1997), préc., note 294, 417.

[326] F. BLANCHETTE, préc., note 236, p. 113 et 114.

[327] 2003 CRTFP 3.

[328] *Id.*, par. 59. Voir également *Commonwealth of Pennsylvania* v. *Proetto,* préc., note 294, par. 19 : « By the very act of sending a communication over the Internet, the party expressly consents to the recording of the message. »; et *United States* v. *Lifshitz*, 369 F.3d 173 (2d Cir. 2004).

réduire l'expectative de vie privée. Tel qu'affirmé par la Cour du district sud de l'Ohio dans l'affaire *United States* v. *Charbonneau*[329], la perte de contrôle de l'expéditeur à l'égard du message dépend plutôt du type de message transmis et de son destinataire[330]. La question que l'on doit se poser n'est donc pas à savoir s'il est techniquement possible de faire suivre le message à des tiers, mais plutôt si l'expéditeur pouvait raisonnablement s'attendre à ce que le destinataire fasse suivre le message à des tiers.

Si par exemple il s'agit d'un message contenant des photographies à caractère pédophile, l'expéditeur ne pourra raisonnablement pas s'attendre à ce que le destinataire ne révèle pas le contenu de son message aux autorités compétentes, par exemple à la police[331]. Dans le contexte du travail, il y a de fortes chances qu'un employé qui reçoit un courriel de cette nature le montre à son employeur. Plus il y a de chances que le message transmis au destinataire soit retransmis à des tiers, moins l'expéditeur pourra prétendre à une expectative raisonnable de vie privée à l'égard du message.

2.2.1.2.2.3.5. Les traces laissées par les activités Internet dans l'ordinateur de l'utilisateur

Tel que mentionné précédemment, toutes les activités Internet laissent des traces dans l'ordinateur de l'utilisateur, et ce, quel que soit le type d'activité. À l'égard des communications Internet, lorsque le message électronique est envoyé ou reçu par le destinataire, il est toujours possible pour des tiers d'en obtenir une copie en accédant à la boîte de courrier électronique ou à la mémoire de l'ordinateur de l'expéditeur ou

---

[329] Préc., note 294.

[330] *Id.*, par. 10-12.

[331] *Warshak* v. *United States*, (6th Cir. 2007), préc., note 256, p. 10 : « [B]y sharing communications with someone else, the speaker or writer assumes the risk that it could be revealed to the government by that person, or obtained through a subpoena directed to that person. See *Miller*, 425 U.S., at 443 ("The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."). »

du destinataire. Ceci est dû au fait que les messages électroniques laissent des traces dans l'ordinateur de l'expéditeur ou du destinataire, que ce soit dans leur boîte de courrier électronique ou dans la mémoire vive de leur ordinateur. Même si l'utilisateur supprime les fichiers contenus dans son ordinateur et vide ensuite le contenu de sa poubelle, les messages électroniques peuvent généralement être retracés. À l'égard de la navigation sur le Web, des traces peuvent également être laissées dans l'ordinateur de l'employé, être retracées et récupérées par l'employeur, tant que l'utilisateur ne vide pas la mémoire cache ou l'historique de navigation dans le contenu de la mémoire de l'ordinateur[332].

Selon la Cour supérieure de Pennsylvanie dans l'arrêt américain *Commonwealth of Pennsylvania* v. *Proetto*[333], cette particularité fait en sorte que la transmission de courrier électronique ou la messagerie instantanée s'apparente à la situation où une personne laisse un message sur une boîte vocale :

> « Sending an e-mail or chat-room communication is analogous to leaving a message on an answering machine. The sender knows that by the nature of sending the communication a record of the communication, including the substance of the communication, is made and can be downloaded, printed, saved, or, in some cases, if not deleted by the receiver, will remain on the receiver's system. Accordingly, by the act of forwarding an e-mail or communication via the Internet, the sender consents by conduct to the recording of the message. »[334]

Dans ce contexte, certains affirment que les traces laissées dans l'ordinateur, tant par les messages électroniques que par la navigation sur le web, peuvent avoir pour effet de diminuer l'expectative de vie privée d'un utilisateur qui ne possède pas un contrôle complet sur son ordinateur.

Toutefois, au même titre que les autres particularités d'Internet, le fait qu'il existe des moyens techniques d'entrer dans la boîte de courrier électronique ou dans la mémoire vive de l'ordinateur d'une personne ne change rien à la nature privée de ces

---

[332] F. BLANCHETTE, préc., note 236, p. 109.

[333] Préc., note 294.

[334] *Id.*, par. 21.

communications ni à l'expectative de vie privée que la personne peut avoir à l'égard de ses communications.

En effet, une personne peut raisonnablement s'attendre, à moins d'être informée du contraire, à ce que les fichiers contenus dans son ordinateur demeurent privés. Évidemment, si l'utilisateur est préalablement informé du fait que l'administrateur du système accédera au réseau pour des raisons déterminées laissant croire à cette personne qu'il accédera à certains fichiers, ou encore si l'utilisateur devait raisonnablement s'attendre à ce que cela puisse se produire, l'expectative raisonnable de vie privée peut en être réduite[335].

L'existence d'un mot de passe personnel secret peut par ailleurs être un facteur important dans l'appréciation de l'expectative raisonnable de vie privée de l'employé à l'égard des fichiers contenus dans son ordinateur et dans sa boîte de courrier électronique[336]. En effet, l'existence d'un mot de passe permet d'empêcher les tiers[337] d'accéder au contenu de l'ordinateur de son travail ou de sa boîte de courriels. Un employé qui détient un mot de passe qui est connu de lui seul peut donc raisonnablement s'attendre à ce que le contenu de son ordinateur et de sa boîte de courriels demeure privé. À cet égard, le mot de passe informatique d'un employé peut se comparer à un cadenas apposé sur un casier privé.

À la lumière de ce qui précède, la question à se poser est à savoir si la personne concernée pouvait raisonnablement s'attendre à ce que ses communications ou l'historique de ses activités sur Internet enregistré sur le réseau soient interceptées, retracées ou récupérées.

2.2.1.2.2.4. *L'environnement de travail*

---

[335] M.-A. POIRIER, préc., note 143, 95.

[336] À titre d'illustration, voir : *United States* v. *Angevine*, préc., note 163; *United States* v. *Long*, préc., note 163; et *United States* v. *Ziegler*, préc., note 163.

[337] À l'exception de l'administrateur du système informatique qui dispose généralement d'un accès à partir du serveur central.

C'est sur le terrain du travail que se posent les principales difficultés liées à l'utilisation des technologies de l'information et des communications et l'expectative raisonnable de vie privée. Dans l'arrêt *R.* c. *Tremblay*[338], la Cour a fait une distinction importante entre l'attente raisonnable de vie privée d'un utilisateur à l'égard du contenu d'un ordinateur personnel se trouvant à la maison et le contenu d'un ordinateur se trouvant sur les lieux du travail :

> « Les arrêts *Gauthier* et *Weir* sont clairs à ce sujet : le contenu d'un ordinateur, en particulier les courriels sont du domaine de la vie privée où il y a une attente raisonnable de vie privée. Mais ces arrêts traitent d'ordinateurs personnels. L'environnement dans lequel est situé l'ordinateur peut aussi avoir une influence sur l'expectative de vie privée au travail ou à la maison. »[339]

Bien qu'une personne puisse disposer d'une expectative raisonnable à la vie privée dans le cadre de l'utilisation d'Internet, il y a de fortes chances que cette expectative soit réduite ou même inexistante du seul fait que cette utilisation est faite dans le contexte ou dans le lieu de travail.

L'environnement de travail présente en effet un certain nombre de circonstances ayant pour effet de réduire l'expectative raisonnable de vie privée des employés dans l'utilisation d'Internet au travail.

2.2.1.2.2.4.1. La propriété des outils informatiques, du courrier électronique et de l'accès Internet

Nous avons mentionné, dans la section 2.1.2.2., que le droit de propriété de l'employeur ne constituait pas, en droit québécois, un fondement du droit de surveillance et qu'il s'agissait plutôt d'un facteur ayant pour effet de réduire le niveau d'expectative de vie privée d'un employé dans l'utilisation de ces outils.

Nous ne reprendrons pas les principes énoncés à la section précédente, compte tenu

---

[338] Préc., note 159.

[339] *Id.*, p. 10.

que ce facteur a été suffisamment exposé précédemment. Nous ne ferons que souligner que bien que le droit de propriété puisse avoir pour effet de réduire l'expectative de vie privée de l'employé, ce facteur doit être utilisé avec réserve. Il ne faut pas uniquement baser l'analyse de l'expectative raisonnable de vie privée sur le droit de propriété de l'employeur, compte tenu de l'importance qui doit être mise sur l'attente subjective de la personne face à la communication en cause, à son caractère raisonnable et à la nature de cette communication. En appliquant par analogie les propos de la Cour d'appel dans l'arrêt *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*[340], la question fondamentale à se poser est à savoir si la communication en tant que telle est protégée plutôt que l'outil de communication[341].

2.2.1.2.2.4.2. La nature du travail exercé par l'employé et la nature de l'entreprise

L'expectative raisonnable de vie privée d'un employé dans l'utilisation d'Internet dépend également du type de travail exercé par l'employé et du type d'entreprise dans lequel celui-ci travaille[342]. En effet, il paraît raisonnable d'affirmer qu'une personne travaillant dans un milieu de travail où les risques et les tentations sont plus grands, ou encore travaillant de la maison, devrait s'attendre à une plus grande surveillance de la part de l'employeur, et donc voir son expectative raisonnable de vie privée diminuée.

D'ailleurs, dans le cadre d'une allocution sur les derniers développements en matière de vie privée au travail tenue à Toronto par le Commissaire à la protection de la vie

---

[340] Préc., note 208.

[341] *Id.*, par. 71.

[342] Par analogie avec les principes reconnus en matière de fouille des employés. On a notamment reconnu qu'un employeur peut plus facilement justifier une fouille des employés s'il exploite une bijouterie (voir à cet effet : *Ambaw et Bijoux Continental Inc.*, D.T.E. 98T-757 (C.T.)) ou encore une mine d'or (voir à cet effet : *Minerais Lac Ltée-La mine Doyon et Métallurgistes unis d'Amérique, section locale 9291*, D.T.E. 93T-928 (T.A.); et *Syndicat des travailleurs de la mine Noranda Inc. Et Métallurgie du cuivre Noranda, fonderie Horne*, D.T.E. 95T-1217 (T.A.)). Dans la doctrine, voir L. BERNIER, L. GRANOSIK et J.-F. PEDNEAULT, préc., note 270, par. 21.120.

privée du Canada, ce dernier a fait une distinction en fonction du type de travail exercé[343] :

> « Un employé dont le travail exige qu'il ait accès à des renseignements secrets ou de nature très délicate (comme moi en tant que commissaire à la protection de la vie privée) devra probablement obtenir une cote sécuritaire, ce qui implique de nombreuses atteintes à la vie privée : une enquête détaillée sur votre passé et votre famille, allant même jusqu'à interroger vos amis et vos anciens patrons.
>
> Mais ces atteintes à la vie privée sont acceptables dans le cas de mon emploi. Elles ne seraient pas acceptables, par contre, dans le cas d'un gérant de banque ou d'un journaliste.
>
> De même, un plus haut niveau de surveillance pourrait se justifier pour les personnes employées dans des milieux de travail où les risques ou les tentations sont exceptionnellement grands. Prenons l'exemple d'une compagnie fabriquant des billets de banques, comparée à une entreprise normale. »[344]

La manière dont le travail est exercé peut également avoir un impact sur l'expectative de vie privée. Depuis quelques années, l'implantation du télétravail a connu une popularité grandissante[345], ce qui a soulevé plusieurs questions au niveau des droits et obligations de l'employeur et de l'employé[346]. Le télétravail est une forme de réalisation de travail suivant laquelle le travail est effectué de façon régulière en dehors des locaux de l'employeur, le plus souvent à domicile, et pour laquelle l'employé fait appel aux technologies de l'information et de la communication fournis par l'employeur pour communiquer à distance[347].

---

[343] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Nouvelle loi, nouvelle époque*, préc., note 219.

[344] *Id.*, p. 6.

[345] S. CÔTÉ, *NETendances 2007, version abrégée,* préc., note 3, p. 57. Selon cette étude, la proportion d'adultes québécois qui ont utilisé Internet pour travailler à la maison à des fins professionnelles a augmenté au fil des années, passant de 19 % en 2004 à 25.7 % en 2007. Voir également : Liette D'AMOURS, « Croissance du télétravail : bonne nouvelle? », *technaute.com*, 28 mars 2007, en ligne : http://technaute.cyberpresse.ca/nouvelles/200703/28/01-11640-croissance-du-teletravail-bonne-nouvelle.php, à l'effet que près de 1,9 million de Québécois utilisent aujourd'hui Internet pour accomplir des tâches professionnelles à domicile.

[346] CEFRIO, *Les enjeux du télétravail au Québec – Rapport de recherche*, Québec, Mai 2001.

[347] OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE (OQLF), « Le grand dictionnaire terminologique », en ligne : http://www.granddictionnaire.com.

De manière générale, la protection du droit à la vie privée est à son apogée lorsqu'une personne se trouve à son domicile, ce qui pourrait laisser croire qu'un télétravailleur dispose d'une plus grande expectative de vie privée qu'un travailleur normal. Jusqu'à maintenant, aucun tribunal québécois ne s'est penché sur la question. Toutefois, tel qu'affirmé par l'ancien Commissaire à la protection de la vie privée du Canada, de par sa nature même, le télétravail exige un niveau de surveillance plus élevé que si l'employé se trouvait dans les locaux de son employeur[348] :

> « De par sa nature même, le télétravail exige probablement plus de surveillance que le travail centralisé. C'est parce que l'employeur n'a pas les moyens normaux de savoir si l'employé travaille toutes les heures pour lesquelles il est payé. (...) Et l'employeur ne peut se contenter de la « tournée du patron » pour veiller à ce que l'employé travaille bel et bien lorsqu'il est au travail. »[349]

Par conséquent, même s'il se trouve à son domicile, le télétravailleur devrait s'attendre à un plus haut niveau de surveillance de la part de son employeur, afin que ce dernier puisse exercer son pouvoir de direction et de contrôle malgré le fait que l'employé ne se trouve pas dans ses locaux.

2.2.1.2.2.4.3. La nature des communications ou des informations surveillées

Afin d'être en mesure d'invoquer une certaine expectative de vie privée à l'égard d'une information transmise ou reçue en milieu de travail, celle-ci doit être de nature personnelle et confidentielle.

Dans l'arrêt *Roy* c. *Saulnier*[350], la Cour d'appel du Québec a affirmé qu'un employé ne disposait d'aucune expectative raisonnable de vie privée à l'égard des conversations d'affaires ou des informations recueillies dans le cadre de son travail à l'aide des systèmes appartenant à l'employeur, compte tenu de la nature

---

[348] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Le respect de la vie privée à l'ère d'Internet*, préc., note 192.

[349] *Id.*, p. 7.

[350] Préc., note 160.

professionnelle de ces conversations.

À l'égard des outils informatiques, les tribunaux québécois favorisent une approche suivant laquelle l'accès à Internet, les ordinateurs et les logiciels fournis par l'employeur constituent avant tout des outils de travail liés à l'exécution de la prestation de travail et que par conséquent, il est raisonnable de présumer que les informations transmises ou reçues par le biais d'Internet sur le lieu de travail sont de nature professionnelle et concernent les affaires de la compagnie. Tel qu'énoncé par la Cour supérieure dans l'affaire *Blais et La Société des Loteries Vidéos du Québec Inc.*[351] :

> « L'employeur fournit l'ordinateur, les logiciels et l'accès Internet afin que l'employé s'en serve dans le cadre de ses fonctions. (...) C'est dire que Sylvain Blais ne pouvait ignorer que le contenu des outils que la SLVQ mettait à sa disposition relevait davantage de sa vie professionnelle que de sa vie privée. »[352]

Cette présomption du caractère professionnel des informations obtenues par le biais des communications effectuées dans le cadre du travail peut néanmoins être renversée, à la charge pour l'employé de prouver, à la lumière des circonstances, que l'employeur pouvait raisonnablement prévoir que la communication ou l'information surveillée était de nature personnelle.

À cet égard, nous pourrions suivre l'approche française, en vertu de laquelle un message comportant expressément dans son objet la mention « personnel », ou encore ayant été classé par l'employé dans un dossier intitulé « personnel », est un message de nature personnelle et confidentielle :

---

[351] Préc., note 136.

[352] *Id.*, par. 95 et 96. Voir également l'affaire *R.* c. *Tremblay* (C.A.), préc., note 159, p. 3 : « Compte tenu de ces éléments de preuve et plus particulièrement du fait que l'appelant soutenait qu'il effectuait l'examen de photographies pornographiques juvéniles dans le cadre d'une enquête, nous sommes d'avis que les fouilles effectuées dans l'ordinateur de l'appelant ne portaient pas atteinte à sa vie privée puisqu'il n'existait aucune expectative de droit à la vie privée en ce qui concernait l'objet même de son travail. »; et *Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada*, préc., note 136, 481 : « Toute cette information se trouvait dans l'outil de travail utilisé, normalement par le plaignant. Dans ces circonstances, il n'était pas illégal, ni abusif, de la part de l'employeur, de vérifier si le plaignant s'était conformé aux exigences du Code d'éthique. » Dans la doctrine, voir : M.-A. POIRIER, préc., note 143, 97.

> « Il doit être généralement considéré qu'un message envoyé ou reçu depuis le poste de travail mis à la disposition par l'entreprise ou l'administration revêt un caractère professionnel, sauf indications manifestes dans l'objet du message ou dans le nom du répertoire où il pourrait avoir été archivé par son destinataire, qui lui conférerait alors le caractère et la nature d'une correspondance privée protégée par le secret des correspondances. »[353]

À l'égard des fichiers ou des dossiers informatiques, l'approche française est également à l'effet que ceux qui sont créés par un employé grâce aux outils informatiques fournis par l'employeur pour l'exécution de son travail sont présumés être de nature professionnelle, à moins d'indications à l'effet contraire dans le nom du répertoire ou du fichier[354].

Suivant cette approche, les tribunaux français ont notamment jugé qu'un employeur ne pouvait fouiller dans les fichiers informatiques d'un employé identifiés comme personnels par ce dernier et contenus sur le disque dur de l'ordinateur mis à sa disposition, à moins que l'employé soit présent ou dûment appelé[355]. À l'égard du courrier électronique, ils ont également considéré qu'une communication était privée dès lors qu'elle était classée dans un répertoire personnel de l'employé, ou encore si l'objet du message faisait apparaître son caractère personnel[356].

Par ailleurs, la présomption du caractère professionnel des informations ou communications transigeant sur le réseau ou sur les ordinateurs appartenant à l'employeur mérite une certaine nuance. Pour les personnes qui passent de

---

[353] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), *La cybersurveillance sur les lieux de travail*, mars 2004, en ligne : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/travail/cyber_conclusions.pdf p. 13. Pour un exposé de l'approche française en matière de surveillance de l'utilisation d'Internet au travail, voir Mathieu MÉLIN et David MELINSON, « Salarié, employeur et données informatiques : brefs regards croisés sur une pièce à succès », *Revue Lamy Droit de l'immatériel*, Janvier 2007, Vol. 23, p. 69.

[354] Colmar, 29 mai 2008, n° 07/03314 (Cour d'appel); Cass. Soc. 18 octobre 2006, pourvoi n° 04-47400; et Cass. Soc. 18 octobre 2006, pourvoi n° 04-48025; et Cass. Soc., 30 mai 2007, pourvoi n° 05-43102.

[355] Soc., 17 mai 2005, *Bull. civ.* V, n° 165 (« Cathnet »). Voir également la décision C.A. Douai (ch. soc.), 30 mars 2007, n° RG 06/02138, dans laquelle un dossier intitulé « jokes » sur le disque dur de l'employé au travail, contenant notamment des vidéos et des photographies à caractère pornographique, a été considéré comme un dossier personnel protégé par la vie privée de l'employé.

[356] Douai, 26 nov. 2004, *M. Philippe X. c/ S.A. Laboratoires Pharmaceutiques Rodael, M. Paul E.*, n° RG 04/00709.

nombreuses heures au travail chaque semaine, il devient inévitable que les outils de travail fournis par l'employeur soient également utilisés à des fins personnelles, comparativement aux personnes qui travaillent une semaine de trente-cinq heures. La Cour d'appel a d'ailleurs considéré cet aspect dans l'arrêt *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*[357], afin de conclure que les conversations en cause, qui avaient eu lieu à partir des appareils téléphoniques appartenant à l'employeur, étaient de nature privée. En l'espèce, l'appelant Sharma, dont la conversation téléphonique avait été interceptée, travaillait des journées entières au temple. Dans les circonstances, la présomption établie dans l'arrêt *Roy* c. *Saulnier*[358] n'était pas applicable[359].

Afin de déterminer la nature des communications ou des informations surveillées, il peut être utile de s'inspirer des lois en matière de protection des renseignements personnels, lesquelles visent essentiellement à protéger la vie privée des individus eu regard aux renseignements personnels qui les concernent. Lorsque l'information est couverte par la notion de « renseignement personnel » telle que définie par les lois applicables, l'employé pourrait alors invoquer une expectative raisonnable de vie privée à l'égard de cette information[360].

L'article 2 Loi sur le secteur privé définit la notion de « renseignement personnel » comme étant « tout renseignement qui concerne une personne physique et permet de l'identifier. ». La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* contient une disposition similaire[361], de

---

[357] Préc., note 208.

[358] Préc., note 160.

[359] *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, préc., note 208, par. 66.

[360] L'expectative raisonnable de vie privée est d'ailleurs l'un des facteurs qui a été considéré par les juges dissidents dans l'arrêt *Dagg* c. *Canada (Ministre des Finances)*, [1997] 2 R.C.S. 403, 437-338, dans le cadre de l'interprétation de la notion de « renseignements personnels ».

[361] Loi sur l'accès, art. 54.

même que les lois fédérales[362].

À première vue, il semblerait que tous les renseignements obtenus par le biais d'une surveillance de l'utilisation d'Internet constituent des renseignements personnels, compte tenu qu'ils peuvent tous se rattacher à un individu. La Cour fédérale du Canada a d'ailleurs affirmé, dans l'affaire *Eastmond* c. *Canadian Pacific Railway*[363], que des renseignements obtenus grâce à une surveillance vidéo sur le lieu de travail constituaient des renseignements personnels au sens de l'article 2 de la L.p.r.p.d.é.

Toutefois, bien que des renseignements puissent incidemment révéler quelque chose au sujet des personnes nommées, ces renseignements ne constituent pas nécessairement des « renseignements personnels » au sens de ces lois[364].

En effet, la définition de « renseignement personnel » dans la L.p.r.p.d.é. exclue expressément le nom, adresse, titre, adresse professionnelle ou numéro de téléphone d'un employé d'une organisation[365]. Par ailleurs, certaines exceptions expressément prévues dans la *Loi sur la protection des renseignements personnels*, établissent clairement une distinction entre les renseignements de nature personnelle et ceux de nature professionnelle ou publique.

L'alinéa 3 (j) de la *Loi sur la protection des renseignements personnels* prévoit notamment que « les renseignements personnels ne comprennent pas les renseignements concernant un cadre ou employé, actuel ou ancien, d'une institution fédérale et portant sur son poste ou ses fonctions »[366]. Cet alinéa précise expressément

---

[362] L.p.r.p.d.é., art. 2 ; et L.p.r.p., art. 3.

[363] 2004 CF 852, en ligne: http://decisions.fct-cf.gc.ca/fr/2004/2004cf852/2004cf852.html.

[364] À titre d'illustration, voir : *Lavoie* c. *Pinkerton du Québec ltée*, [1996] C.A.I. 67, 72 et 73.

[365] C'est-à-dire tout ce qui se trouve en principe sur une carte d'affaire d'un employé. Toutefois, l'adresse de courriel au travail d'une personne constitue un renseignement personnel en vertu de la L.p.r.p.d.é. Voir à cet effet : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2005-297 – *Courriels non sollicités pour fins de marketing*, en ligne : http://www.privcom.gc.ca/cf-dc/2005/297_050331_01_f.asp.

[366] Pour l'équivalent dans la Loi sur l'accès, voir les articles 53, 55, 57 al. 1, paragraphes 1° et 2° et 58.

que le nom d'un employé, lorsqu'il est rattaché à un document établi dans le cours de l'emploi, ou encore les idées et les opinions personnelles qu'un employé a exprimées au cours de son emploi, constituent des renseignements portant sur le poste ou les fonctions de l'employé, et ne sont pas couverts par la notion de « renseignement personnel ».

Dans l'arrêt *Dagg* c. *Canada (Ministre des Finances)*[367], la Cour suprême du Canada est venue préciser la portée de cette exception, en énonçant que des « renseignements qui concernent principalement des personnes elles-mêmes ou la manière dont elles choisissent d'accomplir les tâches qui leur sont confiées sont des « renseignements personnels »[368], et non des renseignements portant sur leur poste ou leurs fonctions[369].

En vertu de ce critère, les renseignements suivants ont été considérés comme des renseignements « portant sur » le poste ou les fonctions de l'employé : i) une feuille contenant le nombre d'heures passées au travail[370]; et ii) les antécédents professionnels d'un employé[371], alors que les documents suivants ont été considérés comme contenant des renseignements personnels : i) un avis disciplinaire[372]; ii) les détails des comptes de dépenses du président d'un organisme public[373] ou les pièces justificatives aux comptes de dépenses[374]; (iii) le rapport de réalisation du projet

---

[367] Préc., note 360.

[368] *Id.*, 407. Bien que les juges de la Cour suprême du Canada aient été divisés quant à l'application du critère, ils se sont quand même entendus à l'unanimité sur l'énoncé du critère (p. 404).

[369] Voir également Colin H.H. MCNAIRN, et Alexander K. SCOTT, *A Guide to the Personal Information Protection and Electronic Documents Act*, Markham (Ont.), Lexis Nexis, 2007, p. 24 : « Information gathered in investigating or evaluating the performance of an employee would likely constitute « personal information » although information about the normal activities of an individual in his or her employment capacity – say opinion expressed by individual in any such role – would not likely constitute « personal information ». »

[370] *Dagg* c. *Canada (Ministre des Finances)*, préc., note 360.

[371] *Canada (Commissaire à l'information)* c. *Canada (Commissaire de la Gendarmerie royale du Canada)*, [2003] 1 R.C.S. 66.

[372] *X. et Komdresco Canada inc.*, D.T.E. 95T-1376 (C.A.I.).

[373] *Laforest* c. *Caisse de dépôt et placement du Québec,* préc., note 219.

[374] *Paquet* c. *Société des alcools du Québec*, [2007] C.A.I. 160 (C.A.I.), conf. par [2008] R.J.D.T. 1079 (C.Q.).

d'année sabbatique de professeurs universitaires[375]; (iv) les relevés de compte du téléphone cellulaire qu'utilise une personne pour son travail[376]; et iv) le nom et l'adresse des établissements où des dépenses d'un cadre sont encourues de même que les service qui ont été obtenus[377].

Par ailleurs, il semblerait que la notion de « renseignement personnel » telle que définie à l'article 2 L.p.r.p.d.é., exclut également les opinions qu'un employé a exprimées dans le cours de son travail[378].

Si nous appliquons ces principes à l'utilisation d'Internet, nous pouvons affirmer que le temps consacré à naviguer sur Internet durant les heures de travail, les fichiers téléchargés à partir d'Internet, ou encore les messages manifestement personnels reçus ou transmis sur le lieu de travail, concernent principalement les employés eux-mêmes et la manière dont ils choisissent d'accomplir leur travail. Il s'agit donc essentiellement de renseignements de nature personnelle à l'égard desquels les employés peuvent raisonnablement s'attendre à ce qu'ils demeurent privés.

À l'opposé, des messages qui seraient transmis par les employés par voie de courrier électronique, contenant par exemple des opinions personnelles ou des idées exprimées dans le cadre de l'exécution de leurs fonctions de travail, ne devraient pas être considérés comme des renseignements personnels. Il s'agirait alors de renseignements portant sur le poste ou les fonctions de l'employé, obtenus dans le cadre de l'exécution du contrat de travail. L'employé ne disposerait d'aucune

---

[375] *Dion-Viens* c. *Université Laval*, [2007] C.A.I. 173, conf. par 2008 QCCQ 640.

[376] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2007-372 – *Les communications aux courtiers en données exposent les faiblesses des mesures de sécurité en télécommunications* – http://www.privcom.gc.ca/cf-dc/2007/372_20070709_f.asp.

[377] *Legris* c. *Repentigny (Ville de)*, [2007] C.A.I. 240 (C.A.I.).

[378] Ian J. TURNBULL, *Privacy in the Workplace : The Employment perspective*, Toronto, CCH, 2004, p. 62.

expectative raisonnable de vie privée à leur égard[379].

Malgré cette distinction quant aux renseignements personnels et non personnels concernant un employé, il ne faut pas oublier, tel qu'exposé dans la section précédente, qu'un employeur est en droit de présumer que les communications transmises ou reçues par le biais des outils informatiques fournis aux employés dans le cadre de leur travail, ou encore les fichiers enregistrés sur le disque dur de l'ordinateur de l'employé, sont de nature professionnelle, d'autant plus que la surveillance est généralement exercée avant de connaître le contenu et la nature des messages ou des fichiers enregistrés. Par conséquent, à moins d'indications claires à l'effet contraire, par exemple dans le nom du fichier, du répertoire, ou encore dans l'objet du message, la présomption du caractère professionnel de l'information ou de la communication ne pourra être renversée.

2.2.1.3. Le droit à la vie privée des tiers

2.2.1.3.1. GÉNÉRALITÉS

Bien que le droit à la vie privée des employés constitue la principale limite au droit de surveillance des employeurs à l'égard de l'utilisation d'Internet, il ne faut pas oublier que d'autres personnes, à l'extérieur de l'entreprise, peuvent également participer aux communications Internet et voir leur droit à la vie privée violé par l'exercice de la surveillance de l'employeur.

En effet, les tiers disposent également d'un droit à la vie privée qui est protégé par les dispositions mentionnées à la section 1.3.1.1. L'employeur doit s'assurer de le respecter.

Dans l'arrêt *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*[380], la Cour d'appel

---

[379] Cette interprétation est d'ailleurs conforme aux principes énoncés dans l'arrêt *Roy* c. *Saulnier*, préc., note 160, à l'effet qu'un employé ne peut s'attendre raisonnablement à ce que des communications d'affaires effectuées dans le cadre de son travail demeurent privées et ne soient pas interceptées par son employeur.

[380] Préc., note 208.

considère d'ailleurs cet aspect dans l'analyse de la recevabilité de la preuve :

> « Il est aussi intéressant de souligner que le juge restreint son analyse à Sharma, toutefois il ne faut pas oublier que le droit à la vie privée de Mme Srivastava fut aussi violé par l'interception illégale de sa conversation. En effet, en mettant l'appareil téléphonique du temple sous écoute, l'intimé s'est donné le pouvoir de s'ingérer dans la vie privée de toutes les personnes qui appelaient au temple durant la période en cause. »[381]

En l'espèce, les conversations interceptées avaient eu lieu entre Sharma, un prêtre embauché par la mission Hindu, et Mme Srivastava, membre de la communauté Hindu. Selon la Cour, le fidèle qui recherche conseil et directive spirituels auprès d'un prêtre jouit d'une assurance quasi constitutionnelle de non-divulgation. Par conséquent, les conversations étaient nécessairement de nature privées.

Dans le dispositif de son jugement, la Cour d'appel a accordé 10,000$ à Mme Srivastava pour compenser le dommage moral qui découlait directement de la violation de sa vie privée.

Par conséquent, un employeur qui décide d'exercer une surveillance de l'utilisation d'Internet au travail doit également faire l'exercice d'évaluer si les tiers qui communiquent avec les employés de son entreprise pour des raisons privées ou confidentielles sont raisonnablement en droit de s'attendre à ce que leurs communications avec les employés de la compagnie demeurent privées.

2.2.1.3.2. LA DÉTERMINATION DE L'EXPECTATIVE RAISONNABLE DE VIE PRIVÉE DES TIERS DANS L'UTILISATION D'INTERNET

À l'égard de l'expectative raisonnable de vie privée des tiers, les principes énoncés dans la section traitant du droit à la vie privée des employés peuvent être transposés et appliqués aux tiers. En effet, à l'exception des facteurs liés à l'environnement de travail, les particularités liées à Internet qui ont un impact sur l'expectative raisonnable de vie privée des personnes qui l'utilisent touchent tout autant les

---

[381] *Id.*, par. 72.

employés que les tiers qui communiquent avec eux par le biais du réseau Internet. En fait, toute personne qui utilise les nouvelles technologies comme moyen de communication se voit soumise à ces facteurs.

De plus, un tiers peut être informé de la surveillance au même titre qu'un employé, par exemple en recevant un avis à cet effet. Le cas échéant, l'expectative de vie privée du tiers pourra également se voir diminué sur la base des principes énoncés dans les sections 2.2.1.2.2.1. à 2.2.1.2.2.3.

Il est important que les employeurs ne négligent pas cet aspect dans le cadre de l'exercice de la surveillance. Si les tiers disposent d'une expectative raisonnable de vie privée dans le cadre de leurs communications avec les employés de la compagnie, la recherche de l'équilibre dans le cadre de l'exercice de la surveillance devra également prendre en considération le droit à la vie privée des tiers.

2.2.2. Le droit à des conditions de travail justes et raisonnables

2.2.2.1. Généralités

L'article 46 de la Charte québécoise garantit à toute personne qui travaille le droit de bénéficier de « conditions de travail justes et raisonnables et qui respectent sa santé, sa sécurité et son intégrité physique ». Ce droit est complété par l'article 2087 C.c.Q. qui s'énonce comme suit :

> « 2087. L'employeur, outre qu'il est tenu de permettre l'exécution de la prestation de travail convenue et de payer la rémunération fixée, doit prendre les mesures appropriées à la nature du travail, en vue de protéger la santé, la sécurité et la dignité du salarié. »

Nous avons vu précédemment que le droit des employés à des conditions de travail justes et raisonnables peut justifier l'exercice d'une surveillance de l'utilisation d'Internet au travail, étant donné les nombreuses situations de harcèlement sexuel et de discrimination qui peuvent surgir en milieu de travail et l'obligation de

l'employeur de prévenir ce genre de situation[382].

Par ailleurs, bien qu'un employeur puisse chercher à assurer à ses employés des conditions de travail justes et raisonnables, de même qu'un environnement de travail exempt de discrimination et de harcèlement, il peut tout autant, par le biais de l'exercice d'une surveillance de l'utilisation d'Internet, porter atteinte à ce droit à l'égard des employés qui sont sujets à la surveillance.

Il est reconnu au Québec que la surveillance électronique peut constituer une violation du droit de l'employé à des conditions de travail justes et raisonnables, tel qu'énoncé dans le contexte d'une surveillance par caméras vidéo dans l'affaire *Liberty Smelting Works (1962) Ltd. et Syndicat international des travailleurs unis de l'automobile, de l'aéronautique, de l'astronautique et des instruments aratoires d'Amérique (T.U.A.)*[383] :

> « Il ne fait aucun doute, dans mon esprit, qu'à moins de dispositions expresses ou implicites au contraire dans la convention, l'employeur ne peut utiliser des circuits de télévisions fermés à des fins disciplinaires ou analogues.
>
> (...)
>
> En tout temps et en tout lieu, il (le travailleur) conserve sa dignité d'homme, sa liberté individuelle.
>
> Il répugne à l'esprit qu'au cours des opérations quotidiennes de son travail il soit constamment sous observation électronique au moyen de caméras braquées sur lui, que tous ses moindres gestes puissent être épiés de façon continue tel un microbe sous un microscope. »[384]

Depuis, et plus particulièrement depuis l'adoption de la Charte québécoise, ce droit a été invoqué à plusieurs reprises afin de contester la surveillance électronique par

---

[382] *Supra*, p. 27 et suiv.

[383] (1972) 3 S.A.G. 1039.

[384] *Id.*, 1044 et 1045. En l'espèce, l'arbitre a restreint l'exercice de la surveillance aux seules fins de la prévention du vol dans l'entreprise et a interdit à l'employeur de fixer l'objectif des caméras de manière constante vers un employé en particulier. À la lecture des propos de l'arbitre, ce n'était pas l'atteinte à la vie privée qui était en cause mais plutôt la dignité de l'employé.

caméra vidéo[385], au niveau de la ligne téléphonique[386] ou des fouilles des employés[387].

Certains considèrent d'ailleurs que l'exercice d'une surveillance électronique, plutôt que de constituer une atteinte à la vie privée de l'employé, constitue plutôt une atteinte au droit à des conditions de travail justes et raisonnables des employés[388]. Cette approche ressort d'ailleurs clairement des propos suivants des auteurs C. D'Aoust, L. Leclerc et G. Trudeau[389] :

> « Il faut donc déterminer si la surveillance électronique *per se* est une condition de travail « raisonnable » et quand elle peut, s'il y a lieu, devenir déraisonnable. Nous soumettons quant à nous qu'il est préférable d'examiner la question à l'étude sous l'angle de la « condition de travail raisonnable » plutôt que par le concept de « droit à la vie privée ». (...)
>
> Nous suggérons (...) qu'une surveillance complète et constante des salariés, sauf exception, constitue une condition de travail déraisonnable, et que l'employeur, s'il l'exerce sans nuance, excède son pouvoir disciplinaire. »[390]

---

[385] À titre d'illustration, voir : *Association des techniciennes et techniciens en diététique du Québec et Centre hospitalier Côte-des-Neiges*, [1993] T.A. 1021, D.T.E. 93T-1329; *Poulies Maska inc. et Syndicat des employés de Poulies Maska inc.*, préc., note 243; *Centre hospitalier de Buckingham et Syndicat des technologues en radiologie du Québec (C.P.S.)*, D.T.E. 2002T-884 (T.A.); *Manufacture de Lambton ltée et Syndicat des salariés de Manufacture Lambton (CSD)*, D.T.E. 2003T-997 (T.A.); *Syndicat des cols bleus regroupés de Montréal, section locale 301 et Montréal (Ville de) (arrondissement Côte-St-Luc—Hampstead—Montréal-Ouest)*, [2005] R.J.D.T. 1068, D.T.E. 2005T-507 (T.A.); *Société des alcools du Québec et Syndicat des travailleuses et travailleurs de la Société des alcools du Québec (SCFP), section locale 3535T*, D.T.E. 2005T-229, AZ-50293590 (T.A.); *Syndicat des travailleuses et travailleurs de la Fabrique Notre-Dame — CSN et Fabrique de la paroisse Notre-Dame*, préc., note 243; *Vifan Canada inc. et Syndicat des travailleuses et travailleurs de Vifan Canada inc. (CSN)*, préc., note 243; et *Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleuses et travailleurs du Canada (TCA-Canada) et Cummins Est du Canada*, [2007] R.J.D.T. 1227, D.T.E. 2007T-678 (T.A.).

[386] À titre d'illustration, voir : *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, préc., note 208.

[387] À titre d'illustration, voir : *Syndicat démocratique des employés de commerce Saguenay-Lac-St-Jean et Potvin & Bouchard inc.*, préc., note 215.

[388] *Société des alcools du Québec c. Syndicat des employés de magasins et de bureaux de la S.A.Q.*, préc., note 237, par. 47 (dans cette dernière affaire, l'arbitre cite d'ailleurs l'affaire *Liberty Smelting Works (1962) Ltd. et Syndicat international des travailleurs unis de l'automobile, de l'aéronautique, de l'astronautique et des instruments aratoires d'Amérique (T.U.A.), local 1470*, préc., note 383); et *Vifan Canada inc. et Syndicat des travailleuses et travailleurs de Vifan Canada inc. (CSN)*, préc., note 243, par. 20.

[389] Claude D'AOUST, Louis LECLERC et Gilles TRUDEAU, *Les mesures disciplinaires : étude jurisprudentielle et doctrinale,* Montréal, École des relations industrielles, Université de Montréal, 1982.

[390] *Id.*, p. 219. Ces propos ont notamment été repris dans l'affaire *Société des alcools du Québec et Syndicat des travailleuses et travailleurs de la Société des alcools du Québec (SCFP), section locale 3535T*, préc., note 385, p. 5.

Il est à noter qu'une politique d'entreprise ou un règlement émis par l'employeur peut constituer une condition de travail[391] et à cet égard peut être considérée comme une condition de travail injuste et déraisonnable au sens de l'article 46 de la Charte québécoise[392].

2.2.2.2. Application en matière de surveillance de l'utilisation d'Internet au travail

En premier lieu, il convient de déterminer si la surveillance de l'utilisation d'Internet constitue une condition de travail. À cet égard, les principes établis en matière de surveillance électronique traditionnelle et en matière de politique de l'utilisation d'Internet au travail ne laissent aucun doute à l'effet que la surveillance de l'utilisation d'Internet constitue une condition de travail.

D'ailleurs, à la lumière de l'affaire *Association des juristes de l'État et Commission des valeurs mobilières du Québec*[393], une politique de l'utilisation d'Internet au travail prévoyant expressément l'existence d'une surveillance constitue une condition de travail, dès lors que la politique déborde le cadre du simple manuel d'utilisation technique d'un outil de travail, et que son contenu est susceptible de faire l'objet d'une négociation entre les parties et d'être intégrées dans une convention collective[394].

À la lumière de ces principes, et par analogie avec les décisions rendues en matière de surveillance électronique, nous pouvons certainement affirmer que la mise en place d'une surveillance de l'utilisation d'Internet constitue une condition de travail, que sa mise en place peut constituer une modification aux conditions de travail et que,

---

[391] *Association des juristes de l'État et Commission des valeurs mobilières du Québec*, [2003] R.J.D.T. 579, D.T.E. 2003T-212 (T.A.).

[392] À titre d'illustration, voir : *Métallurgistes unis d'Amérique, section locale 9414 et Nettoyeur Shefford inc.*, préc., note 245. En l'espèce, l'employeur avait adopté une politique à l'effet qu'il ne payait plus ses employés le temps pendant lequel ceux-ci étaient aux toilettes. Selon l'arbitre, cette politique constituait une condition de travail déraisonnable au sens de l'article 46 de la Charte québécoise.

[393] Préc., note 391.

[394] *Id.*, par. 65 et 66.

dépendamment de la manière dont elle est exercée ou de son caractère raisonnable dans les circonstances, elle pourrait être considérée comme une condition de travail injuste et déraisonnable en violation de l'article 46 de la Charte québécoise[395].

Par ailleurs, les politiques de surveillance de l'utilisation d'Internet peuvent également être considérées comme des conditions de travail injustes et déraisonnables, si elles ne poursuivent pas un but légitime ou si la surveillance en vertu de la politique est exercée de manière déraisonnable. Les politiques de surveillance prévoient généralement, et ce, de façon détaillée, la manière dont la surveillance sera exercée, la procédure suivie avant, pendant et après la surveillance, de même que les personnes en charge de la surveillance au sein de l'entreprise. Il pourrait arriver qu'un ou plusieurs aspects de la procédure prévue dans la politique porte atteinte au droit des employés à des conditions de travail justes et raisonnables.

Dans l'affaire, *Association des juristes de l'État et Commission des valeurs mobilières du Québec*[396], l'arbitre n'a pas à se pencher sur cet aspect en profondeur, mais devait par ailleurs déterminer si l'économie générale de la politique Internet permettait de l'associer à une norme de saine gestion ou à un impératif circonstanciel. À cet égard, l'arbitre a conclu positivement en affirmant ce qui suit :

> « [L]e but évident de la politique dans son ensemble apparaît être clairement de s'assurer que toute utilisation des ressources informatiques de la Commission soit compatible avec la mission de l'organisme, respectueuse de son image publique et conforme à ses responsabilités et obligations, que ce soit en termes de légalité, d'éthique, de civilité, de productivité, de confidentialité, de discrimination, de sécurité ou d'intégrité tant du matériel informatique que des ressources d'information qui font l'objet de son utilisation. (...) En effet, on peut reconnaître qu'un employeur ait apporté des modifications aux conditions de travail de ses salariés dans le cours normal de ses affaires, en l'occurrence pour tenir compte de l'impact de l'évolution technologique (...). »[397]

Pour que l'exercice ou les politiques de surveillance n'entraînent pas des conditions

---

[395] Louise LAPLANTE, « L'Internet et l'emploi » dans S.F.P.B.Q., *Congrès annuel du Barreau du Québec (1997)*, Cowansville, Éditions Yvon Blais, p. 709, à la page 723.

[396] Préc., note 391.

[397] *Id.*, par. 98-100.

de travail injustes et déraisonnables, l'employeur doit donc avoir des motifs pour exercer la surveillance et celle-ci doit être exercée de manière raisonnable[398]. Pour y arriver, l'employeur doit remplir un certain nombre de conditions et suivre une certaine procédure, de manière à conserver un équilibre entre ses droits, ceux des employés et ceux des tiers.

Dans le troisième chapitre, nous verrons comment, en pratique, l'employeur peut exercer une telle surveillance de l'utilisation d'Internet par les employés, sans que cela constitue une atteinte à leur droit à la vie privée ou à leur droit à des conditions de travail justes et raisonnables, ou encore une atteinte au droit à la vie privée des tiers.

---

[398] *Association des techniciennes et techniciens en diététique du Québec et Centre hospitalier Côte-des-Neiges*, préc., note 385, 1028 et 1029.

3. GUIDE PRATIQUE POUR LA MISE EN PLACE D'UNE SURVEILLANCE

Dans le cadre du deuxième chapitre, nous avons vu que le droit de surveillance de l'employeur, découlant de son pouvoir de direction et de contrôle, pouvait se heurter au droit à la vie privée des employés ou des tiers. Nous avons également vu qu'en plus du droit à la vie privée, le droit de surveillance pouvait se heurter au droit des employés de jouir de conditions de travail justes et raisonnables.

Dans le cadre du présent chapitre, nous verrons comment un employeur peut mettre en place une surveillance de l'utilisation d'Internet de ses employés tout en contrebalançant les différents intérêts en jeu. À cet égard, la détermination de l'expectative raisonnable de vie privée du ou des employés soumis à la surveillance, de même que l'analyse préalable des critères de rationalité et de proportionnalité, sont deux étapes essentielles à la mise en place d'une surveillance de l'utilisation d'Internet au travail, et ce afin d'être en mesure de délimiter cette balance des intérêts et de définir les droits et obligations de l'employeur vis-à-vis des employés et des tiers.

Nous verrons que dans tous les cas, l'employeur doit respecter les critères du droit de surveillance, et plus particulièrement :

a) déterminer les fins de la surveillance de l'utilisation d'Internet au travail et s'assurer que celles-ci respectent le critère de rationalité;

b) se demander si la surveillance est nécessaire et si un moyen moins intrusif que la surveillance de l'utilisation d'Internet pourrait lui permettre d'atteindre ces fins; et

c) déterminer comment il exercera la surveillance de manière à porter le moins possible atteinte aux droits des personnes surveillées (préférablement recueillir le moins de renseignements personnels possible sur un individu).

Par ailleurs, à la lumière de l'analyse de l'expectative raisonnable de vie privée et des critères du droit de surveillance, nous verrons que dans certains cas, l'employeur doit, préalablement à l'implantation de la surveillance, respecter un certain nombre d'obligations, plus particulièrement :

d) informer les employés et les tiers surveillés de l'existence et de l'étendue de la surveillance de l'utilisation d'Internet; et

e) obtenir le consentement des employés surveillés quant à l'exercice de la surveillance.

Dans ce contexte, l'employeur a intérêt à adopter une politique de surveillance de l'utilisation d'Internet, même s'il ne s'agit pas là d'une obligation légale ni d'une condition à l'exercice de la surveillance.

L'employeur peut également être sujet à d'autres obligations, notamment en ce qui a trait à la protection des renseignements personnels[399]. Nous nous limiterons toutefois à approfondir les obligations les plus importantes et qui soulèvent le plus d'interrogations lors de la mise en place d'une surveillance de l'utilisation d'Internet au travail.

Voyons maintenant plus en détails en quoi consistent ces différents critères et obligations.

3.1. Les critères du droit de surveillance

3.1.1. Généralités

Pour que la surveillance de l'utilisation d'Internet au travail soit exercée tout en conservant un équilibre entre les divers intérêts concurrents, deux critères doivent être respectés : (i) le critère de rationalité ; et (ii) le critère de proportionnalité. Ces critères

---

[399] L'employeur doit être transparent dans le cadre de la surveillance. Voir le 8e principe (Transparence) de l'annexe 1 de la L.p.r.p.d.é. qui énonce plusieurs mesures permettant d'assurer la transparence au niveau de la gestion des renseignements personnels. Voir également L.p.r.p.d.é., annexe 1, principe 4.1.4c).

permettent d'apprécier la légalité de l'atteinte à la vie privée ou le caractère raisonnable de la surveillance comme condition de travail, afin de déterminer si l'employeur a le droit de surveiller ses employés.

À cet égard, il est important de bien comprendre que, dans tous les cas, ces deux critères doivent être respectés. Ainsi, même si les employés ont connaissance de la surveillance et ont consenti à cette mesure, l'employeur demeure soumis aux deux critères tout au long de la surveillance.

À ce jour, aucun tribunal québécois n'a analysé la surveillance de l'utilisation d'Internet au travail à la lumière de ces critères[400]. Le fait que le droit à la vie privée ou à des conditions de travail justes et raisonnables n'ait que très rarement été soulevé en matière de surveillance de l'utilisation d'Internet ou de l'équipement informatique au travail[401] ne contribue d'ailleurs pas à développer le droit jurisprudentiel en la matière. Pourtant, ces critères sont appliqués tant en matière de surveillance vidéo[402],

---

[400] Dans deux décisions, les tribunaux ont conclu que l'employé ne disposait pas, en l'espèce, d'une attente raisonnable de vie privée dans le cadre des activités Internet surveillées : *Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada*, préc., note 136; et *Blais et La Société des Loteries Vidéos du Québec Inc.,* préc., note 136. Dans deux autres décisions, les tribunaux ont conclu que l'employé ne disposait pas, en l'espèce, d'une attente raisonnable de vie privée à l'égard du contenu de son ordinateur : *Syndicat des professionnelles et professionnels des affaires sociales du Québec (C.S.N.) et Institut de réadaptation en déficience physique de Québec*, préc., note 154; et *Ghattas* c. *École nationale de théâtre du Canada*, préc., note 167.

[401] *Id.*

[402] L'arrêt-clé en matière de surveillance vidéo est : *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 117. Voir également *Association des techniciennes et techniciens en diététique du Québec et Centre hospitalier Côte-des-Neiges*, préc., note 385; *Bombardier inc. — Canadair et Association internationale des machinistes et des travailleurs de l'aérospatiale, loge d'avionnerie de Montréal, section locale 712*, [1996] T.A. 251, D.T.E. 96T-375; *Union des routiers, brasserie, liqueurs douces et ouvriers de diverses industries, section locale 1999 et Brasserie Labatt ltée (Montréal)*, [1999] R.J.D.T. 648, D.T.E. 99T-402 (T.A.); *Syndicat canadien des communications, de l'énergie et du papier et Induspac, division Corrugué inc.*, préc., note 215; *Unidindon inc. et Syndicat des travailleurs d'abattoir de volaille de St-Jean-Baptiste (C.S.N.)*, préc., note 215; *Garaga inc. et Syndicat des salariés de garage (C.S.D.)*, [2002] R.J.D.T. 1802, D.T.E. 2002T-1100 (T.A.); *Syndicat national des employés de garage du Québec inc. et Sovea Auto ltée*, D.T.E. 2002T-707, AZ-02141190 (T.A.), conf. par (C.A., 2003-10-21), 200-09-004301-021, SOQUIJ AZ-03019685; *Syndicat des cols bleus regroupés de Montréal, section locale 301 (S.C.F.P.) et La Ronde (Six Flags)*, D.T.E. 2004T-1124 (T.A.); *Société des alcools du Québec et Syndicat des travailleuses et travailleurs de la Société des alcools du Québec (SCFP), section locale 3535T*, préc., note 385; *Syndicat des employés de l'aluminerie de Baie-Comeau (CSN) et Alcoa ltée (Aluminerie de Baie-Comeau)*, D.T.E. 2005T-608, AZ-50319506 (T.A.); *Syndicat des employées et employés de la Société des casinos du Québec, section unité générale (CSN) et Société des casinos du Québec*, D.T.E. 2006T-394, AZ-55000105 (T.A.); *Genest et Québec (Directeur général des élections)*, D.T.E. 2007T-167 (C.F.P.); *Poulies Maska inc. et Syndicat des employés de*

d'écoute téléphonique[403] qu'en matière de fouille au travail[404]. La surveillance de l'utilisation d'Internet au travail pouvant constituer tant une atteinte aux droits fondamentaux des employés qu'au droit à des conditions de travail justes et raisonnables, il n'y a aucun motif pour ne pas appliquer ces critères en matière de surveillance de l'utilisation d'Internet des employés. Les principes énoncés dans le présent chapitre découlent dès lors principalement d'analogies avec les principes reconnus en matière de surveillance traditionnelle et de fouille au travail.

Afin de bien comprendre les critères de rationalité et de proportionnalité, il convient en premier lieu d'exposer leurs fondements. Ces critères découlent en effet d'une série de dispositions législatives et de l'interprétation qu'en ont donnée les tribunaux.

3.1.2. La source des critères

3.1.2.1. Le droit à la vie privée

Lorsque la ou les personnes surveillées disposent d'une expectative raisonnable de vie privée, l'employeur doit s'assurer de respecter les dispositions relatives à la vie privée.

Poulies Maska inc., préc., note 243; *Syndicat de l'enseignement des Deux Rives (SEDR-CSQ) et Commission scolaire des Navigateurs*, préc., note 215; *Syndicat des travailleurs unis du Québec — STUQ (FTQ) et Pomatek inc.*, préc., note 215; *Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleuses et travailleurs du Canada et BMW Canbec*, préc., note 215; *Vifan Canada inc. et Syndicat des travailleuses et travailleurs de Vifan Canada inc. (CSN)*, préc., note 243; *Syndicat national des travailleurs des pâtes et papiers de Donnacona inc. (CSN) et Produits forestiers Alliance inc. (Bowater)*, préc., note 243; et *Syndicat des employées et employés de métiers d'Hydro-Québec, section locale 1500 — SCFP (FTQ) et Hydro-Québec,* D.T.E. 2009T-273 (T.A.).

[403] *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, préc., note 208; *Ste-Marie* c. *Placements JPM Marquis inc.*, préc., note 216; *Syndicat des salariées et salariés de La Survivance et La Survivance*, préc., note 216.

[404] *Entreprises Cara Ltée et Association internationale des machinistes et des travailleurs de l'aéroastronautique, loge 987*, [1984] T.A. 10, D.T.E. 84T-26; *Canapar Ltée et Fraternité nationale des charpentiers-menuisiers, forestiers, travailleurs d'usines*, [1985] T.A. 606, D.T.E. 85T-755; *Syndicat des travailleurs de l'énergie et de la chimie, section locale 107* c. *Laurin*, préc., note 272; *Syndicat démocratique des employés de commerce Saguenay-Lac-St-Jean et Potvin & Bouchard inc.*, préc., note 215; COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Fouilles des véhicules et effets personnels de travailleurs à la sortie d'une mine – compatibilité avec la Charte des droits et libertés de la personne*, Cat. 2.115.11, Québec, Juin 1998, en ligne : http://www.cdpdj.qc.ca/fr/publications/docs/fouilles_vehicules.pdf, p. 8; Yves SAINT-ANDRÉ, « Le respect du droit à la vie privé au travail : mythe ou réalité? », dans S.F.P.B.Q., vol. 205, *Développements récents en droit du travail (2004),* Cowansville, Éditions Yvon Blais, p. 51, à la page 60; et Benoît TURMEL, « Le droit de fouille en milieu de travail » dans Denis NADEAU et Benoit PELLETIER (dir.), *Relation d'emploi et droits de la personne; évolution et tensions!,* Actes du colloque de la faculté de droit de l'Université d'Ottawa tenu le 12 mars 1993, Cowansville, Éditions Yvon Blais, 1994, p. 51.

À cet égard, certaines dispositions permettent aux employeurs de porter atteinte à la vie privée des personnes et c'est dans ce contexte que les critères de rationalité et de proportionnalité interviennent : une atteinte à la vie privée sera permise si cette atteinte respecte les critères de rationalité et de proportionnalité.

L'une des dispositions d'où découlent ces critères est l'article 1 de la Charte canadienne qui s'énonce comme suit :

> « 1. La *Charte canadienne des droits et libertés* garantit les droits et libertés qui y sont énoncés. Ils ne peuvent être restreints que par une règle de droit, dans des limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique. »

Les arrêts clés *R.* c. *Oakes*[405] et *R.* c. *Edwards Books and Art Ltd.*[406] ont d'ailleurs bien établi que l'article 1 de la Charte canadienne impliquait les critères de rationalité et de proportionnalité :

> « Pour établir qu'une restriction est raisonnable et que sa justification peut se démontrer dans le cadre d'une société libre et démocratique, il faut satisfaire à deux exigences. En premier lieu, l'objectif législatif que la restriction vise à promouvoir doit être suffisamment important pour justifier la suppression d'un droit garanti par la Constitution. Il doit se rapporter à des "préoccupations urgentes et réelles". En second lieu, les moyens choisis pour atteindre ces objectifs doivent être proportionnels ou appropriés à ces fins. La proportionnalité requise, à son tour, comporte normalement trois aspects : les mesures restrictives doivent être soigneusement conçues pour atteindre l'objectif en question, ou avoir un lien rationnel avec cet objectif; elles doivent être de nature à porter le moins possible atteinte au droit en question et leurs effets ne doivent pas empiéter sur les droits individuels ou collectifs au point que l'objectif législatif, si important soit-il, soit néanmoins supplanté par l'atteinte aux droits. La Cour a affirmé que la nature du critère de proportionnalité pourrait varier en fonction des circonstances. Tant dans son élaboration de la norme de preuve que dans sa description des critères qui comprennent l'exigence de proportionnalité, la Cour a pris soin d'éviter de fixer des normes strictes et rigides. »[407]

Bien que cette disposition s'applique uniquement aux lois et règlements adoptés par des organismes gouvernementaux et puisse difficilement s'appliquer à l'égard d'une mesure

---

[405] [1986] 1 R.C.S. 103.

[406] [1986] 2 R.C.S. 713.

[407] *Id.*, 768 et 769.

de surveillance prise par un employeur[408], il est néanmoins utile de s'inspirer de ses principes et interprétations pour apprécier la légalité d'une surveillance de l'utilisation d'Internet.

Au Québec, la disposition équivalente à l'article 1 de la Charte canadienne qui autorise les atteintes aux droits fondamentaux sous réserve des critères de rationalité et de proportionnalité est l'article 9.1 de la Charte québécoise qui s'énonce comme suit :

> « 9.1. Les libertés et les droits fondamentaux s'exercent dans le respect des valeurs démocratiques, de l'ordre public et du bien-être général des citoyens du Québec. La loi peut, à cet égard, en fixer la portée et en aménager l'exercice. »

Les décisions ayant appliqué l'article 9.1 de la Charte québécoise illustrent la similarité des critères développés en vertu de cette disposition et de ceux développés en vertu de l'article premier de la Charte canadienne. Les tribunaux ont d'ailleurs affirmé à plusieurs reprises que l'article 9.1 de la Charte québécoise devait être interprété et appliqué de la même manière que l'article premier de la Charte canadienne, ou encore prendre appui sur cette disposition[409]. Par conséquent, tel qu'énoncé par la Cour suprême du Canada dans l'arrêt *Godbout* c. *Ville de Longueuil*[410], la partie qui invoque l'article 9.1 pour justifier une atteinte aux droits et libertés fondamentaux a la charge d'établir que les critères de rationalité et de proportionnalité sont respectés :

---

[408] La décision d'un organisme soumis à la *Charte canadienne* de soumettre des employés à une surveillance pourra être considérée comme une règle de droit au sens de la Charte seulement si elle est expressément prévue par une disposition ou une politique législative. Voir par analogie l'arrêt *Multani* c. *Commission scolaire Marguerite-Bourgeoys*, [2006] 1 R.C.S. 256, par. 112-125; et Henri BRUN et Guy TREMBLAY, *Droit constitutionnel*, 5e éd., Cowansville, Éditions Yvon Blais 2008, p. 932.

[409] *Ford* c. *Québec (Procureur général)*, [1988] 2 R.C.S. 712, par. 63; *Godbout* c. *Ville de Longueuil*, préc., note 172, par. 104; *Section locale 143 du Syndicat canadien des communications, de l'énergie et du papier* c. *Goodyear Canada inc.*, [2008] R.J.D.T. 24, J.E. 2008-97 (C.A.), p. 5; COMMISSION DES DROITS DE LA PERSONNE ET DE LA JEUNESSE, *Filature et surveillance des salariés absents pour raison de santé : conformité à la charte*, Cat. 2.115.21, Québec, Avril 1999, en ligne : http://www.cdpdj.qc.ca/fr/publications/docs/filature.pdf, p. 10 et 11; et André LAJOIE, *Pouvoir disciplinaire et tests de dépistages de drogues en milieu de travail: illégalité ou pluralisme*, Cowansville, Éditions Yvon Blais, 1995, p. 56.

[410] Préc., note 172.

> « Ainsi que la Cour l'a expliqué dans l'arrêt *Ford*, la partie qui invoque l'art. 9.1 pour tenter de justifier la limitation d'un droit garanti par la *Charte* québécoise a donc la charge de prouver que cette limite est imposée dans la poursuite d'un objectif légitime et important et qu'elle est proportionnelle à cet objectif, c'est-à-dire qu'elle est rationnellement liée à l'objectif et que l'atteinte au droit est minimale; voir l'arrêt *Oakes*, précité, et l'arrêt *R. c. Edwards Books and Art Ltd.*, [1986] 2 R.C.S. 713. »[411]

Comme le droit à la vie privée est l'un des droits fondamentaux garantis par la Charte québécoise, l'employeur québécois qui entend surveiller l'utilisation d'Internet doit respecter les critères de l'article 9.1 lorsque ses employés ou les tiers impliqués disposent d'une expectative raisonnable de vie privée dans le cadre de leurs activités Internet.

Les critères de l'article 9.1 ont d'ailleurs été appliqués à l'égard de différents types de surveillance, notamment en matière de surveillance par caméras vidéo[412] et de mise sous écoute des conversations téléphoniques des employés[413].

L'application des critères de rationalité et de proportionnalité est également illustrée en matière de protection des renseignements personnels dans le cadre de la justification de la collecte, de l'utilisation ou de la communication des renseignements collectés. Tel que mentionné précédemment, la surveillance de l'utilisation d'Internet implique souvent la collecte, l'utilisation et la communication de renseignements personnels[414]. Le cas échéant, l'employeur doit s'assurer de respecter les dispositions prévues dans les lois sur la protection des renseignements

---

[411] *Id.*, par. 104.

[412] *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 117; *Syndicat canadien des communications, de l'énergie et du papier et Induspac, division Corrugué inc.*, préc., note 215; *Unidindon inc. et Syndicat des travailleurs d'abattoir de volaille de St-Jean-Baptiste (C.S.N.)*, préc., note 215; *Syndicat national des employés de garage du Québec inc. et Sovea Auto ltée*, préc., note 402; *Syndicat des employées et employés de la Société des casinos du Québec, section unité générale (CSN) et Société des casinos du Québec*, préc., note 402; *Genest et Québec (Directeur général des élections)*, préc., note 402; *Syndicat des travailleurs unis du Québec — STUQ (FTQ) et Pomatek inc.*, préc., note 215; *Syndicat national des travailleurs des pâtes et papiers de Donnacona inc. (CSN) et Produits forestiers Alliance inc. (Bowater)*, préc., note 243; et *Syndicat des employées et employés de métiers d'Hydro-Québec, section locale 1500 — SCFP (FTQ) et Hydro-Québec*, préc., note 402.

[413] *Ste-Marie c. Placements JPM Marquis inc.*, préc., note 216; et *Syndicat des salariées et salariés de La Survivance et La Survivance*, préc., note 216.

[414] *Supra*, p. 63.

personnels.

À cet égard, tant l'article 37 C.c.Q, les articles 4 et 5 Loi sur le secteur privé, l'article 64 Loi sur l'accès, que l'article 5(3) L.p.r.p.d.é. imposent un critère de nécessité ou de fins raisonnables dans le cadre de la collecte, de l'utilisation ou de la communication de renseignements personnels.

Il est par ailleurs reconnu que l'exigence de nécessité qui se retrouve dans les lois québécoises en matière de protection des renseignements personnels s'interprète au regard des critères de rationalité et de proportionnalité. Ce principe a notamment été affirmé dans l'affaire *Laval (Société de transport de la Ville de)* c. *X.*[415], dans laquelle la Cour du Québec a affirmé que le critère de nécessité prévu dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* devait être interprétée d'une manière qui soit conforme aux exigences de la Charte québécoise[416]. En vertu du principe que l'article 9.1 de la Charte québécoise devait être appliqué de la même manière que l'article premier de la Charte canadienne, elle a ajouté que la meilleure façon d'interpréter cette disposition consistait à interpréter l'exigence de nécessité en fonction des deux volets du critère établis par la Cour suprême du Canada dans l'arrêt *R.* c. *Oakes*[417], soit l'existence d'un objectif important et la proportionnalité des moyens en cause au regard de cette atteinte

Bien que l'affaire *Laval (Société de transport de la Ville de)* c. *X.*[418] ait été rendue dans le contexte de la Loi sur l'accès, la Cour du Québec a estimé que la Loi sur l'accès et la Loi sur le secteur privé reprenaient le même concept de « nécessité »[419]. D'ailleurs, selon la Cour supérieure du Québec, les décisions et interprétations

---

[415] Préc., note 285.

[416] *Id.*, par. 38.

[417] Préc., note 405.

[418] Préc., note 285.

[419] *Id.*, par. 32.

rendues dans le contexte de la Loi sur l'accès s'appliquent aux fins de l'interprétation de la Loi sur le secteur privé[420].

Par ailleurs, plusieurs décisions en matière de collecte de renseignements personnels ont interprété le mot « nécessaire » de l'article 5 de la Loi sur le secteur privé comme devant être interprété de manière restrictive, et dans le sens de « requis, indispensable , obligatoire », et non pas simplement d'« utile »[421]. Cette interprétation illustre l'importance d'avoir un intérêt légitime et sérieux lors de la collecte de renseignements personnels sur un individu, de même que l'importance d'établir la nécessité de l'atteinte.

Quant aux lois fédérales sur la protection des renseignements personnels, les mêmes principes ressortent. En effet, dans l'affaire *Eastmond* c. *Canadian Pacific Railway*[422], la Cour fédérale devait déterminer si la surveillance par caméra vidéo exercée par l'employeur à l'égard de ses employés respectait les dispositions de la L.p.r.p.d.é., particulièrement l'art. 5(3)[423]. Dans sa décision, la Cour fédérale du Canada a confirmé que le test permettant de déterminer si les fins poursuivies pour la collecte de renseignements personnels étaient raisonnablement acceptables au sens de cette disposition se divisait en quatre critères :

> « -La mesure est-elle manifestement nécessaire pour répondre à un besoin particulier?
> -Est-il probable qu'elle répondra efficacement à ce besoin?

---

[420] *Personnelle-vie (La), corp. d'assurances* c. *Cour du Québec*, [1997] R.J.Q. 2296, 2303.

[421] *Bellerose* c. *Université de Montréal*, [1986] C.A.I. 109, 113, conf. par J.E. 89-350, [1988] C.A.I. 377 (C.Q.); *Syndicat des employées et employés professionnels et de bureau, section locale 57 et Caisse populaire St-Stanislas de Montréal*, préc., note 241, 365; *Regroupement des Comités Logement et Association de locataires du Québec c. Corporation des propriétaires immobiliers du Québec, rapport d'enquête*, [1995] C.A.I. 370 (C.A.I.), AZ-95151509, p. 16; *Praderes* c. *Les Immeubles de la Montagne Ste-Catherine (1974) inc.*, PV 97 17 29, 4 avril 2001 (C.A.I.); *Gauthier* c. *Nautilus Plus*, PV 98 14 62, 12 février 2002 (C.A.I.), p. 5; Karl DELWAIDE et Antoine AYLWIN, « Leçons tirées de dix ans d'expérience : La Loi sur la protection des renseignements personnels dans le secteur privé du Québec », *Conférence juridique canadienne et l'exposition commerciale de l'Association du Barreau canadien*, Vancouver, Colombie-Britannique, 16 août 2005, en ligne : http://www.priv.gc.ca/information/pub/dec_050816_f.pdf, p. 13.

[422] Préc., note 363.

[423] L.p.r.p.d.é., art. 5(3): « L'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. »

> -La perte de vie privée est-elle proportionnelle à l'avantage obtenu?
> -Existe-t-il un moyen qui porte moins atteinte à la vie privée et permette d'arriver au même but? »[424]

Les deux premiers critères décrits dans cette décision équivalent au critère de rationalité, alors que les deux derniers équivalent au critère de proportionnalité. Ce test, qui a été confirmé à plusieurs reprises par le Commissariat à la protection de la vie privée du Canada en matière de surveillance par caméras vidéo[425], doit également s'appliquer en matière de surveillance de l'utilisation d'Internet lorsqu'il s'agit de se conformer aux dispositions de la L.p.r.p.d.é.

3.1.2.2. Le droit à des conditions de travail justes et raisonnables

Les critères de rationalité et de proportionnalité sont également appliqués afin d'apprécier si une condition de travail est juste et raisonnable[426]. Sans y être mentionnés expressément, ils ressortent clairement des décisions québécoises relatives au droit à des conditions de travail justes et raisonnables en matière de surveillance traditionnelle[427] et de fouille[428], et notamment des propos de l'arbitre Me

---

[424] *Eastmond* c. *Canadian Pacific Railway*, préc., note 363, par. 13.

[425] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumés de conclusions d'enquêtes en vertu de la LPRPDÉ : n° 2003-114 – *Un employé s'oppose à l'utilisation de caméras vidéo numériques de surveillance par la compagnie*, en ligne : http://www.priv.gc.ca/cf-dc/2003/cf-dc_030123_f.cfm; n° 2004-264 – *Caméras vidéo et cartes magnétiques au travail*; n° 2004-265 – *Caméras vidéo au travail,* en ligne : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040219_02_f.cfm; n° 2004-269 – *L'employeur embauche un enquêteur privé pour exercer une surveillance vidéo d'un employé,* en ligne : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040423_f.cfm; n° 2004-273 – *À la suite de l'installation de caméras de surveillance sur les lieux de travail, une compagnie de radiodiffusion s'engage à informer ses employés des fins de la collecte et à adopter une politique concernant leur utilisation,* en ligne : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040518_f.cfm; n° 2004-279 – *La surveillance des employés au travail,* en ligne : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040219_01_f.cfm; et n° 2005-290 – *La surveillance des employés au travail,* en ligne : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040726_f.cfm; et n° 2007-379 – *L'état des toilettes amène la direction d'une entreprise à y exercer une surveillance,* en ligne : http://www.priv.gc.ca/cf-dc/2007/379_20070404_f.cfm.

[426] Pour un exposé du droit à des conditions de travail justes et raisonnable, voir *supra*, section p. 115.

[427] En matière de surveillance vidéo, voir : *Association des techniciennes et techniciens en diététique du Québec et Centre hospitalier Côte-des-Neiges*, préc., note 385; *Union des routiers, brasserie, liqueurs douces et ouvriers de diverses industries, section locale 1999 et Brasserie Labatt ltée (Montréal)*, préc., note 402; *Poulies Maska inc. et Syndicat des employés de Poulies Maska inc.*, préc., note 243; *Garaga inc. et Syndicat des salariés de garage (C.S.D.)*, préc., note 402; *Société des alcools du Québec et Syndicat des travailleuses et travailleurs de la Société des alcools du Québec (SCFP), section locale 3535T*, préc., note 385; *Syndicat des cols bleus regroupés de Montréal, section locale 301 et Montréal (Ville de) (arrondissement Côte-St-Luc—Hampstead—Montréal-Ouest)*, préc., note 385; *Syndicat national de l'automobile, de l'aérospatiale, du*

Carol Jobin dans l'affaire *Syndicat des cols bleus regroupés de Montréal, section locale 301 et Montréal (Ville de) (arrondissement Côte-St-Luc—Hampstead—Montréal-Ouest)*[429] :

> « Il n'est pas interdit à la Ville d'installer des caméras de surveillance en permanence à l'extérieur et à l'intérieur de ses bâtiments pour protéger les biens et les personnes à titre préventif
>
> Ce qui est interdit parce qu'il s'agit d'une condition de travail déraisonnable, c'est que ces caméras de surveillance soient constamment braquées sur des individus, épiant ainsi systématiquement leurs faits et gestes. Il s'agit alors d'une forme de harcèlement au même titre que si un contremaître s'installait en permanence auprès d'un salarié pour le surveiller pendant toute la durée de son travail.
>
> Tel que mentionné plus haut, un employeur peut néanmoins avoir recours à des caméras de surveillance dans des circonstances particulières qui le justifient. Il doit exister un problème substantiel et continu qui fasse que l'installation de caméras soit rendue nécessaire et que cette caméra soit utilisée de façon cohérente et proportionnée par rapport au problème à solutionner et de façon à ne fixer un salarié en permanence. »[430]

De même que des propos de l'arbitre Me Jean-Denis Gagnon dans l'affaire *Association des techniciennes et techniciens en diététique du Québec et Centre hospitalier Côte-des-Neiges*[431] qui, dans l'application de l'article 46 de la Charte, affirme ce qui suit :

> « Si l'existence de vols dans son établissement justifiait l'employeur d'avoir recours à un mode de surveillance électronique du lieu où il croyait qu'ils survenaient, il lui

---

transport et des autres travailleuses et travailleurs du Canada et BMW Canbec, préc., note 215; *Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleuses et travailleurs du Canada (TCA-Canada) et Cummins Est du Canada*, préc., note 385; *Syndicat des travailleurs unis du Québec — STUQ (FTQ) et Pomatek inc.*, préc., note 215; *Vifan Canada inc. et Syndicat des travailleuses et travailleurs de Vifan Canada inc. (CSN)*, préc., note 243; et en matière d'écoute téléphonique : *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, préc., note 208; et *Syndicat des salariées et salariés de La Survivance et La Survivance*, préc., note 216; et.

[428] *Syndicat des travailleurs de l'énergie et de la chimie, section locale 107* c. *Laurin*, préc., note 272; *Syndicat démocratique des employés de commerce Saguenay-Lac-St-Jean et Potvin & Bouchard inc.*, préc., note 215; et L. BERNIER, L. GRANOSIK et J.-F. PEDNEAULT, préc., note 270, par. 21.070 à 21.136.

[429] Préc., note 385.

[430] *Id.*, 1081 (nos soulignés). Voir également *Vifan Canada inc. et Syndicat des travailleuses et travailleurs de Vifan Canada inc. (CSN)*, préc., note 243.

[431] Préc., note 385.

> incombait d'utiliser ce moyen afin seulement d'atteindre le but légitime qu'il poursuivait – faire cesser les vols - et d'une manière qui porte le moins possible atteinte au droit des requérantes d'exercer leurs fonctions sans être assujetties à un guet constant. »[432]

Bien qu'aucun tribunal québécois n'ait encore appliqué ces critères en matière de surveillance de l'utilisation d'Internet au travail, il apparaît évident, par analogie avec les décisions précitées, que les critères de rationalité et de proportionnalité s'appliquent à l'analyse de la surveillance de l'utilisation d'Internet au regard du droit à des conditions de travail justes et raisonnables.

Maintenant que nous avons exposé la source des critères de rationalité et de proportionnalité, voyons maintenant en quoi consistent ces critères et comment ils doivent s'appliquer en matière de surveillance de l'utilisation d'Internet.

3.1.3. L'application des critères

3.1.3.1. Le critère de rationalité

3.1.3.1.1. GÉNÉRALITÉS

Le critère de rationalité fait référence à l'objectif poursuivi par l'employeur. Pour satisfaire à ce critère, l'employeur doit viser, par le biais de l'obligation ou de la mesure imposée, à atteindre un ou des objectifs légitimes et importants. Il ne faut donc pas que la surveillance constitue une « expédition de pêche ». Il faut éviter que les renseignements collectés par le biais de la surveillance n'aient aucune pertinence quant à l'atteinte d'un objectif légitime et important de l'employeur.

Le critère de rationalité se divise en trois parties. La première partie vise à s'assurer que les fins de la mesure prise par l'employeur existent au moment de la mise en place de la surveillance; la deuxième partie analyse la légitimité des fins de la surveillance au regard des intérêts que l'employeur cherche à protéger; et la troisième partie analyse l'importance des fins de la surveillance au regard des incidents subis ou

---

[432] *Id.*, 1028 (nos soulignés).

des doutes soulevés par l'employeur.

À l'égard de la légitimité et de l'importance des fins, il est important de comprendre que le degré de légitimité et d'importance requis pour que les objectifs invoqués satisfassent au critère de rationalité dépend notamment : (i) du niveau d'expectative de vie privée de l'employé; et (ii) de la manière dont l'employeur entend exercer la surveillance de l'utilisation d'Internet.

En effet, moins le niveau d'expectative de vie privée du ou des employés surveillés est élevé, moins le niveau de légitimité et d'importance requis est sévère. Par conséquent, si les employés ont été informés de la surveillance et ont donné leur consentement, l'employeur aura en principe plus de facilité à satisfaire au critère de rationalité.

Par ailleurs, plus la manière dont l'employeur entend exercer la surveillance de l'utilisation d'Internet porte atteinte aux droits des employés ou encore s'assimile à une forme de harcèlement, plus les fins soulevées par l'employeur pour justifier sa surveillance devront être légitimes et importantes.

Tel que nous le verrons dans la section 3.2.1.3.[433], il existe des situations dans lesquelles les fins soulevées par l'employeur sont suffisamment légitimes et importantes pour lui permettre d'exercer la surveillance sans le consentement et à l'insu de l'employé, et ce malgré le fait que la surveillance porte atteinte à la vie privée de l'employé. Ce sera notamment le cas si l'employeur subit de sérieux problèmes en lien avec l'utilisation d'Internet au travail, ou s'il entretient de sérieux doutes quant à des activités illégales menées sur Internet par un employé au travail.

3.1.3.1.1.1. *La période de référence*

En premier lieu, pour que les fins poursuivies par l'employeur répondent au critère de

---

[433] *Infra*, p. 166.

rationalité, elles doivent exister avant ou à tout le moins au moment de la mise en place de la surveillance[434]. Elles ne peuvent être crées *a posteriori*, soit après que la surveillance ait été effectuée[435], ni démontrer une intention de se défaire d'un employé pour des raisons non justifiées.

Ce principe est notamment appliqué dans l'affaire *Mascouche (Ville de)* c. *Houle*[436]. En l'espèce, la mise sous écoute et l'enregistrement des conversations téléphoniques de Mme Houle avaient été effectuées par un voisin curieux sans raison précise autre que par simple curiosité. Il n'existait, au moment de la mise sous écoute et de l'enregistrement des conversations téléphoniques de Mme Houle, aucun soupçon à son égard ni aucune raison de vouloir la soumettre à une telle surveillance. Toutefois, l'écoute des conversations téléphoniques avait permis au voisin de découvrir des activités déloyales de la part de Mme Houle vis-à-vis son employeur, la Ville de Mascouche. Le voisin était donc allé voir l'employeur de Mme Houle avec les enregistrements pour lui dénoncer les actes déloyaux de l'employée. La Ville a par la suite congédié Mme Houle et a tenté de produire en preuve les enregistrements électroniques.

La Cour d'appel a confirmé la décision de la Cour supérieure à l'effet de rejeter la prétention de la Ville suivant laquelle la seule façon de savoir si la preuve avait été obtenue en portant atteinte à la vie privée de Mme Houle était d'écouter les enregistrements. Selon la Cour, la preuve par écoute téléphonique avait été obtenue illégalement en raison du contexte dans lequel les enregistrements avaient été faits, soit en portant atteinte à la vie privée de l'employé, et « un contrôle ex post facto (...) permettait d'une part que la violation du droit se perpétue et, d'autre part, que la

---

[434] *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 117, 1089; *Syndicat des employées et employés de la Société des casinos du Québec, section unité générale (CSN) et Société des casinos du Québec*, préc., note 402, p. 50; et Y. SAINT-ANDRÉ, préc., note 404, à la page 67.

[435] *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 117, 1089.

[436] Préc., note 234.

justice soit déconsidérée »[437].

Afin de déterminer si une surveillance a été exercée en portant atteinte à la vie privée de la personne surveillée, il faut donc évaluer les conditions dans lesquelles la surveillance a été effectuée plutôt que le contenu du résultat de la surveillance. Les objectifs de la mesure portant atteinte à la vie privée doivent exister avant ou au moment de la mise en place de la surveillance. Ce principe concorde d'ailleurs avec le deuxième principe de l'annexe 1 de la L.p.r.p.d.é. qui s'énonce comme suit : « Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci. ».

3.1.3.1.1.2. *La légitimité des fins*

Par ailleurs, tel que mentionné précédemment, le ou les objectifs poursuivis par l'employeur dans le cadre d'une surveillance des employés doivent être légitimes. La légitimité de l'objectif fait référence aux intérêts que l'employeur cherche à protéger. Pour être légitime, l'objectif recherché doit être lié au bon fonctionnement de l'entreprise. Tel qu'énoncé dans l'arrêt *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*[438], « [i]l faut d'abord que l'on retrouve un lien entre la mesure prise par l'employeur et les exigences du bon fonctionnement de l'entreprise ou de l'établissement en cause. Il ne saurait s'agir d'une décision purement arbitraire et appliquée au hasard. »[439]

Le niveau de légitimité d'un objectif varie en fonction de son rapprochement avec les intérêts économiques de l'entreprise. Plus l'objectif visé touche les intérêts économiques de l'employeur, moins il sera considéré comme légitime :

---

[437] *Id.*, 1915. Bien que dans la décision de la Cour supérieure du Québec, celle-ci ait fait une distinction entre les faits en l'espèce et les situations de surveillance au travail, le principe à l'effet que les fins poursuivies par l'employeur doivent exister avant la mise en place de la surveillance doit également s'appliquer en matière de surveillance au travail.

[438] Préc., note 117.

[439] *Id.*, 1089. Voir également *Syndicat des travailleurs unis du Québec — STUQ (FTQ) et Pomatek inc.*, préc., note 215, par. 34.

> « Lorsqu'il est question de la protection des lieux, des biens ou des personnes, l'employeur a certainement un intérêt légitime à exercer une surveillance vigilante à cet égard. Ces situations ne relèvent pas seulement des intérêts de l'employeur, mais aussi de l'ordre public. Il en va de même lorsque l'honnêteté de la personne salariée est en cause. Toutefois, lorsque l'employeur poursuit des objectifs strictement d'ordre économique en s'intéressant au rendement des personnes salariées en vue de la rentabilité de son entreprise, la situation paraît différente. (...) Néanmoins, l'objectif de rentabilité concerne surtout les intérêts personnels de l'employeur. Il paraît donc avoir moins de poids quant à sa légitimité que l'objectif visant à assurer la protection et la sécurité des biens ou des personnes. »[440]

La Cour fédérale avait d'ailleurs rappelé, dans l'arrêt *Eastmond* c. *Canadian Pacific Railway*[441] le fait que l'utilisation de caméras de surveillance pour enregistrer la productivité des employés était généralement condamnée par les tribunaux[442]. Ce principe doit toutefois être considéré avec réserve, compte tenu qu'il existe des situations dans lesquelles les problèmes de productivité subis par l'employeur sont suffisamment sérieux et dommageables pour justifier une atteinte aux droits des employés. Ce sera notamment le cas si les propres clients de l'employeur se plaignent de la mauvaise qualité et des retards du service.

À titre d'illustration, dans *Syndicat des travailleurs unis du Québec – STUQ (FTQ) et Pomatek inc.*[443], l'employeur avait créé un quart de soir en raison du nombre important de plaintes de clients concernant la qualité des services de l'entreprise. Or, malgré cette mesure, la situation ne s'était pas améliorée. L'employeur avait donc décidé de mettre en place une surveillance vidéo de ses salariés travaillant sur le quart de soir. À la lumière de la preuve, l'arbitre a donné raison à l'employeur et a reconnu que ce dernier entretenait des doutes suffisamment sérieux pour lui permettre d'adopter la mesure de surveillance.

---

[440] D. VEILLEUX, préc., note 241, à la page 37. À titre d'illustration, voir : *Poulies Maska inc. et Syndicat des employés de Poulies Maska inc.*, préc., note 243, p. 9; *Société des alcools du Québec et Syndicat des travailleuses et travailleurs de la Société des alcools du Québec (SCFP), section locale 3535T*, préc., note 385, par. 20; et *Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleuses et travailleurs du Canada et BMW Canbec*, préc., note 215, par. 43.

[441] Préc., note 363.

[442] *Id.*, par. 133.

[443] Préc., note 215.

3.1.3.1.1.3. *L'importance des fins*

En plus d'être légitime, l'objectif visé par le biais de la surveillance doit être important. L'importance d'un objectif sera établie si l'employeur démontre qu'il a des motifs de croire qu'un ou des employés commettent une faute et que l'atteinte aux droits de la personne concernée est nécessaire dans les circonstances.

L'importance de l'objectif dépend en grande partie des incidents subis par l'employeur, des doutes qu'il entretient sur certains employés, et de l'impact que ces incidents ou ces risques d'incidents peuvent avoir sur l'organisme qu'il exploite.

À cet égard, une simple allégation ou un simple doute quant au comportement de l'employé ne reposant sur aucun motif sérieux ne peut suffire pour établir l'importance de l'objectif poursuivi[444]. L'intérêt soulevé doit être fondé sur des motifs raisonnables qui justifient l'utilisation de ce moyen de surveillance. Les motifs de l'employeur peuvent notamment provenir d'une plainte déposée au sein de l'entreprise quant au comportement d'un employé[445], d'un incident, d'informations découvertes par inadvertance, l'important étant que la surveillance ne soit pas exercée de manière systématique.

---

[444] *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 117, 1089; et B. TURMEL, préc., note 404, à la page 61. Pour des illustrations jurisprudentielles de motifs suffisamment sérieux en matière de surveillance vidéo, voir : *Association des techniciennes et techniciens en diététique du Québec et Centre hospitalier Côte-des-Neiges*, préc., note 385; *Syndicat national des employés de garage du Québec inc. et Sovea Auto ltée*, préc., note 402; *Syndicat des employés de l'aluminerie de Baie-Comeau (CSN) et Alcoa ltée (Aluminerie de Baie-Comeau)*, préc., note 402; *Syndicat des employées et employés de la Société des casinos du Québec, section unité générale (CSN) et Société des casinos du Québec*, préc., note 402; *Genest et Québec (Directeur général des élections)*, préc., note 402; *Syndicat des travailleurs unis du Québec — STUQ (FTQ) et Pomatek inc.*, préc., note 215; *Syndicat des employées et employés de métiers d'Hydro-Québec, section locale 1500 — SCFP (FTQ) et Hydro-Québec*, préc., note 402; Pour des illustrations jurisprudentielles de doutes n'étant pas suffisamment sérieux en matière de surveillance vidéo, voir : *Syndicat canadien des communications, de l'énergie et du papier et Induspac, division Corrugué inc.*, préc., note 215; *Unidindon inc. et Syndicat des travailleurs d'abattoir de volaille de St-Jean-Baptiste (C.S.N.)*, préc., note 215; *Garaga inc. et Syndicat des salariés de garage (C.S.D.)*, préc., note 402; *Syndicat de l'enseignement des Deux Rives (SEDR-CSQ) et Commission scolaire des Navigateurs*, préc., note 215; et *Syndicat national des travailleurs des pâtes et papiers de Donnacona inc. (CSN) et Produits forestiers Alliance inc. (Bowater)*, préc., note 243.

[445] *Briar* c. *Conseil du Trésor (Solliciteur général du Canada - Service correctionnel)*, préc., note 327, par. 59 : « Moreover, the employer's investigation was driven by a complaint on which it was bound do act. This is not a case of random surveillance. »

Si par ailleurs les soupçons de l'employeur se basent sur son jugement subjectif plutôt que sur des preuves tangibles, l'usage de la surveillance pour évaluer le comportement de l'employé sera jugé injustifié et disproportionné par rapport aux intérêts de l'employé[446].

L'arrêt *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*[447], en matière de surveillance par caméras vidéo, illustre bien ce principe. En l'espèce, l'employeur cherchait à vérifier la loyauté d'un employé absent pour cause de maladie et avait mis en place un système de filature vidéo à l'extérieur du lieu de travail. La Cour a conclu que l'employeur avait des motifs sérieux de douter de l'honnêteté du comportement de l'employé, compte tenu d'un diagnostic médical erroné et de plusieurs contradictions manifestes dans le comportement de l'employé. Il ne s'agissait donc pas de doutes superficiels.

À l'opposé, dans une affaire impliquant des faits similaires[448], l'arbitre a conclu au caractère déraisonnable de la surveillance vidéo. L'appréciation des objectifs de la surveillance demeure donc du cas par cas. En l'espèce, les faits allégués par l'employeur pour établir ses doutes vis-à-vis la loyauté de l'employé se résumaient à deux appels anonymes dénonçant le fait que le plaignant, en congé de maladie, travaillait ailleurs. Selon l'arbitre, bien que ces deux appels fussent susceptibles de créer des doutes, il ne s'agissait pas de doutes suffisamment sérieux pour justifier qu'on porte atteinte à la vie privée de l'employé.

En matière de protection des biens appartenant à l'employeur, l'appréciation de l'objectif tiendra compte des incidents subis par l'employeur, et du caractère actuel et continu du problème occasionné. La nécessité de mettre en place une mesure de

---

[446] À titre d'illustration en matière de surveillance vidéo, voir : *Syndicat de l'enseignement des Deux Rives (SEDR-CSQ) et Commission scolaire des Navigateurs*, préc., note 215.

[447] Préc., note 117. Voir également *Syndicat des employés municipaux de la Ville de Saguenay (CSN) et Saguenay (Ville de)*, préc., note 243; *Genest et Québec (Directeur général des élections)*, préc., note 402.

[448] *Unidindon inc. et Syndicat des travailleurs d'abattoir de volaille de St-Jean-Baptiste (C.S.N.)*, préc, note 215.

surveillance pour protéger les biens de l'employeur sera établie si des vols, actes de vandalismes ou tout autre acte portant atteinte à la propriété de l'employeur sont survenus récemment chez l'employeur, rendant ainsi la surveillance nécessaire pour enrayer le problème en question. L'employeur pourra par ailleurs difficilement justifier une atteinte aux droits des personnes concernées si un seul incident est survenu dans le passé ou encore si la période de temps écoulée depuis le dernier incident ne permet plus d'établir l'existence d'un problème actuel et continu[449].

3.1.3.1.2. L'APPLICATION EN MATIÈRE DE SURVEILLANCE DE L'UTILISATION D'INTERNET

Par analogie avec les principes précités, il apparaît donc que pour établir l'importance de l'objectif dans le contexte d'une surveillance de l'utilisation d'Internet, l'employeur qui entend exercer une surveillance doit s'assurer que les risques invoqués sont non seulement présents, mais existent de manière suffisamment importante pour justifier de porter atteinte à la vie privée des employés par le biais de la surveillance.

En matière de surveillance de l'utilisation d'Internet, les objectifs soulevés par l'employeur doivent avoir un lien avec un ou plusieurs des avantages ou désavantages exposés au premier chapitre relativement à l'utilisation d'Internet au sein des entreprises[450]. Tous ces avantages ou désavantages contribuent ou nuisent au bon fonctionnement de l'entreprise, que ce soit au niveau de la performance, de la productivité, de l'image, de la protection de ses informations confidentielles, de la sécurité de ses données, de la responsabilité juridique ou des pertes financières de

---

[449] À titre d'illustration en matière de surveillance vidéo, voir : *Union des routiers, brasserie, liqueurs douces et ouvriers de diverses industries, section locale 1999 et Brasserie Labatt ltée (Montréal)*, préc. note 402 (les caméras ont été installées trois semaines après le principal acte de vandalisme et deux semaines après la fin des négociations et la signature de la convention collective; le tribunal a conclu qu'au moment où les caméras vidéo ont été installées, il n'existait plus de problème nécessitant un tel mode de surveillance); et *Syndicat des cols bleus regroupés de Montréal, section locale 301 (S.C.F.P.) et La Ronde (Six Flags)*, préc., note 402 (évènement circonstanciel survenu lors de la Fête du Canada, un an avant l'installation des caméras; le tribunal d'arbitrage a conclu que rien ne démontrait l'existence d'un problème actuel et continu à l'endroit où les caméras avaient été installées).

[450] *Supra*, p. 8 et suiv.

l'entreprise.

Toutefois, il ne faut pas croire qu'un objectif, dès qu'il est lié à ces risques et avantages, est dès lors suffisamment légitime pour justifier une surveillance au niveau de l'utilisation d'Internet. Certains objectifs seront suffisamment légitimes dans certaines circonstances et ne le seront pas dans d'autres. Selon le type d'entreprise, du type de travail effectué par l'employé et de l'environnement dans lequel travaille l'employé, la légitimité des risques variera. De même, si l'employeur a mis en place un système de filtrage des contenus pouvant entrer ou sortir sur le réseau, certains risques, par exemple la circulation de contenus illégaux sur le réseau, se verront grandement diminués.

Pour satisfaire au critère de rationalité en présence d'un intérêt purement économique, l'employeur devra prouver l'existence d'un problème sérieux spécifique lié à la productivité ou à la qualité du travail des employés, plutôt qu'un simple problème potentiel, de même qu'un impact important pour l'organisme. Ce principe ressort clairement des propos de l'ancien Commissaire à la protection de la vie privée du Canada lors d'une allocution donnée en 2002[451] :

> « Ce ne sont pas là des préoccupations banales. Les employeurs doivent être en mesure de s'assurer que leurs employés ne magasinent pas en ligne alors qu'ils devraient travailler. (...) Si un employeur prouve qu'il y a des problèmes spécifiques à l'un ou l'autre de ces aspects, il peut avoir satisfait au premier critère. Mais je recommande toujours aux employeurs de ne pas spéculer ou généraliser à propos d'un « problème potentiel ». Je pense que vous devriez raisonnablement vous attendre à ce qu'un employeur prouve qu'il existe un problème réel et précis. »[452]

Si la surveillance est instaurée uniquement comme moyen de prévention, par exemple pour prévenir le vol de temps des employés utilisant Internet à des fins personnelles durant les heures de travail, la rationalité de l'atteinte sera difficile à établir, au même titre que si l'entreprise cherche uniquement, par le biais de la surveillance, à

---

[451] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La vie privée au travail à l'ère d'Internet*, préc., note 1.

[452] *Id.*, p. 6.

sauvegarder son image ou sa réputation, compte tenu qu'il s'agit encore là d'intérêts purement économiques.

Les objectifs visés par le biais d'une surveillance de l'utilisation d'Internet n'ont pas tous un caractère purement économique. En effet, tel qu'exposé au premier chapitre, l'employeur se doit, dans certaines matières, d'être proactif et de prendre des mesures concrètes pour prévenir des situations préjudiciables. C'est notamment le cas en matière de harcèlement sexuel et de protection des informations confidentielles. Compte tenu par exemple de l'augmentation des risques de harcèlement sexuel avec l'apparition d'Internet au travail, une surveillance exercée au niveau du courrier électronique ou de la messagerie instantanée en vue de prévenir les situations de harcèlement sexuel pourra être reconnue comme une mesure raisonnable adoptée par l'employeur. Si l'employeur invoque ces obligations pour justifier sa surveillance de l'utilisation d'Internet, la légitimité de l'objectif sera plus facile à établir.

Le même raisonnement s'applique pour les entreprises qui traitent des renseignements personnels et qui ont des obligations légales importantes à l'égard de leur conservation et de leur divulgation. Compte tenu que ces entreprises doivent prendre des mesures adéquates afin d'assurer la sécurité des renseignements personnels, une entreprise qui gère un volume important de renseignements personnels sera justifiée d'exercer une surveillance de l'utilisation d'Internet au travail afin de s'assurer que les informations personnelles qu'elle détient demeurent protégées et que leur confidentialité est préservée.

Par ailleurs, dépendamment du degré d' importance requis à l'égard des objectifs invoqués, l'employeur devra être en mesure de prouver la survenance d'incidents, par exemple des situations d'importantes baisses de productivité, de violations de droits d'auteur commises par les employés par le biais d'Internet au travail ou de dissémination d'informations privilégiées sur l'entreprise. La nécessité de la surveillance devra dans certains cas être fondée sur des soupçons réels et substantiels, appuyée sur des preuves sérieuses, récentes, à l'effet qu'un employé en particulier se livre à des pratiques préjudiciables, illégales ou interdites par l'employeur par le biais

de l'utilisation d'Internet.

En somme, le respect du critère de rationalité dans le cadre d'une surveillance au travail dépend de chaque cas d'espèce et doit être appréciée en tenant compte de nombreux facteurs[453]. Dans chaque cas d'espèce, il s'agit de déterminer si les risques invoqués sont réellement présents, préalablement à l'exercice de la surveillance, et ce, à la lumière des facteurs suivants :

- le type d'entreprise exploitée par l'employeur;
- le type d'employés embauchés (professionnels ou ouvriers);
- le type de travail effectué par les employés;
- le contexte et l'environnement dans lequel travaillent les employés (bureaux fermés ou ouverts, discipline stricte ou détendue, filtrage ou non filtrage);
- les incidents ou expériences subies dans le passé par l'employeur, les soupçons qu'il entretient sur le comportement des employés dans le cadre de l'utilisation d'Internet au travail, et les éléments de faits à la base de ses soupçons;
- les personnes pouvant bénéficier de la mesure de surveillance; et
- le lien entre l'objectif et les intérêts économiques de l'entreprise.

3.1.3.2. Le critère de proportionnalité

3.1.3.2.1. GÉNÉRALITÉS

Quant au critère de proportionnalité, celui-ci concerne plus particulièrement le choix des moyens. À cet égard, nous pouvons nous référer plus particulièrement aux propos

---

[453] *Godbout* c. *Ville de Longueuil*, préc., note 174, par. 4 : « Ces critères doivent être appliqués avec souplesse et d'une manière adaptée au contexte particulier et aux circonstances factuelles de chaque espèce. Il se peut qu'un objectif suffisamment impérieux dans un cas ne respecte pas la norme dans un contexte différent. »

de la Cour d'appel dans l'arrêt *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*[454] énoncés en matière de filature des employés :

> « Au niveau du choix des moyens, il faut que la mesure de surveillance, notamment la filature, apparaisse comme nécessaire pour la vérification du comportement du salarié et que, par ailleurs, elle soit menée de la façon la moins intrusive possible. Lorsque ces conditions sont réunies, l'employeur a le droit de recourir à des procédures de surveillance, qui doivent être aussi limitées que possible. »[455]

Le critère de proportionnalité se divise en deux parties. La première partie concerne le choix de la mesure prise par l'employeur pour atteindre son objectif et analyse la nécessité et l'efficacité de l'atteinte aux droits des employés. La deuxième partie concerne l'exécution de la mesure et vise à s'assurer que celle-ci porte le moins possible atteinte aux droits des personnes assujetties.

3.1.3.2.1.1. *La nécessité et l'efficacité de l'atteinte*

La mesure ou l'obligation imposée par l'employeur doit apparaître comme nécessaire pour résoudre efficacement le problème de l'employeur ou pour atteindre ses objectifs légitimes et importants[456], le but étant d'éviter de porter inutilement atteinte à la dignité ou à la vie privée d'un salarié.

Pour que la mesure apparaisse comme nécessaire, l'employeur doit être en mesure de démontrer qu'elle offre un degré d'efficacité propre pour justifier l'atteinte aux droits des employés assujettis. En d'autres mots, l'employeur ne doit disposer d'aucune autre solution de remplacement efficace et raisonnable pour atteindre son objectif, ou encore il doit avoir épuisé toutes les autres solutions de remplacement efficaces et

---

[454] Préc., note 117.

[455] *Id.*, 1089.

[456] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La vie privée au travail à l'ère d'Internet*, préc., note 1, p. 7.

raisonnables à sa disposition[457]. Il n'est toutefois pas requis que la surveillance soit l'unique moyen à la disposition de l'employeur.

L'employeur pourrait par exemple, plutôt que d'instaurer une surveillance au travail, afficher des avis ou des annonces qui traitent du problème, faire de la formation à l'interne pour sensibiliser les employés au problème, ou encore donner à certains membres du personnel un rôle de surveillance. De telles mesures, pourraient, dans certaines circonstances, permettre à l'employeur d'arriver au même résultat, et ce d'une manière qui porte moins atteinte à la vie privée des employés. Si l'employeur n'a pas épuisé tous ces recours, il lui sera difficile d'établir que la surveillance constitue la mesure nécessaire et efficace pour résoudre efficacement le problème de l'employeur ou pour atteindre ses objectifs légitimes et importants[458].

Le coût des différentes solutions à la disposition de l'employeur pour remédier son problème constitue également un facteur pouvant être pris en compte dans l'appréciation de la nécessité et de l'efficacité de l'atteinte, compte tenu qu'il joue un rôle dans le caractère raisonnable du choix des moyens. Par conséquent, si un moyen moins intrusif existe, mais que les coûts reliés à l'implantation de ce moyen sont non négligeables par rapport à son efficacité, le moyen plus intrusif, mais beaucoup moins coûteux, pourrait être considéré comme une mesure efficace et raisonnable pour

---

[457] Pour des illustrations jurisprudentielles de ce principe appliqué en matière de surveillance vidéo, voir : *Bombardier inc. — Canadair et Association internationale des machinistes et des travailleurs de l'aérospatiale, loge d'avionnerie de Montréal, section locale 712*, préc., note 402; *Syndicat des cols bleus regroupés de Montréal, section locale 301 et Montréal (Ville de) (arrondissement Côte-St-Luc—Hampstead—Montréal-Ouest)*, préc., note 385; *Syndicat des employés de l'aluminerie de Baie-Comeau (CSN) et Alcoa ltée (Aluminerie de Baie-Comeau)*, préc., note 402; *Syndicat des employées et employés de la Société des casinos du Québec, section unité générale (CSN) et Société des casinos du Québec*, préc., note 402; *Syndicat de l'enseignement des Deux Rives (SEDR-CSQ) et Commission scolaire des Navigateurs*, préc., note 215; *Syndicat des travailleurs unis du Québec — STUQ (FTQ) et Pomatek inc.*, préc., note 215; *Vifan Canada inc. et Syndicat des travailleuses et travailleurs de Vifan Canada inc. (CSN)*, préc., note 243;. En matière de protection des renseignements personnels, voir : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumés de conclusions d'enquêtes en vertu de la LPRPDÉ : n° 2004-268 - *La surveillance électronique ne donne aucun résultat, mais la pratique est fortement découragée,* en ligne : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040412_f.cfm; et n° 2007-379, préc., note 425.

[458] À titre d'illustration en matière de surveillance vidéo, voir : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumés de conclusions d'enquêtes en vertu de la LPRPDÉ : n° 2004-268, préc., note 457; et n° 2004-279, préc., note 425; et n° 2007-379, préc., note 425.

résoudre le problème[459]. Toutefois, pour reprendre les propos de l'arbitre Me Fernand Morin dans l'affaire *Syndicat de l'enseignement des Deux Rives (SEDR-CSQ) et Commission scolaire des Navigateurs*[460], si l'employeur a choisi un « moyen apparemment financièrement moins coûteux mais professionnellement plus odieux»[461], la mesure sera vue comme étant disproportionnée par rapport à l'objectif recherché.

3.1.3.2.1.1. Le caractère minime de l'atteinte

Non seulement la surveillance doit apparaître comme une solution efficace et nécessaire, mais elle doit être menée de la manière la moins intrusive possible, de façon à ne pas brimer inutilement les droits de ses employés[462]. Même si l'employeur a des motifs sérieux et légitimes de vouloir procéder à une surveillance, l'atteinte à la vie privée doit être minimale eu égard aux circonstances. Le mode de surveillance mis en œuvre par l'employeur doit être « raisonnable, approprié»[463] quant à son étendue au regard de l'objectif poursuivi par l'employeur[464], doit l'être de façon à porter le moins possible atteinte à la vie privée, à la dignité, à l'intégrité et à la liberté des employés[465].

À cet égard, une surveillance exercée de manière constante ou systématique sera généralement considérée comme disproportionnée par rapport à l'objectif

---

[459] À titre d'illustration en matière de surveillance vidéo, voir : *Société des alcools du Québec et Syndicat des travailleuses et travailleurs de la Société des alcools du Québec (SCFP), section locale 3535T*, préc., note 385, par. 57.

[460] Préc., note 215.

[461] *Id.*, p. 14.

[462] *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 117, 1089.

[463] *R.* c. *M. (M.R.)*, préc., note 233, p. 423.

[464] D. VEILLEUX, préc., note 241, 44.

[465] K. DELWAIDE, « L'Internet en milieu de travail et les politiques et directives relatives à l'utilisation des nouvelles technologies », préc., note 53, p.38; R. PERREAULT, préc., note 111, à la page 91; et D. VEILLEUX, préc., note 241, 43.

recherché[466], à moins que des faits particuliers justifient ou rendent nécessaire cette surveillance continue[467].

Les propos du Commissaire à la protection de la vie privée du Canada à l'occasion d'une allocution sur la surveillance de la vie privée au travail illustrent d'ailleurs les méfaits d'une surveillance exercée de manière continue et sans discrimination[468] :

> « La surveillance continuelle et sans discrimination des employés, ajoute-t-elle, traduit un manque de confiance et fait peser le soupçon sur tous les employés alors que les problèmes peuvent être attribuables à quelques personnes ou à un mode de gestion éventuellement contestable. Elle estime que ce genre de mise en observation omniprésente peut entraver les comportements indésirables mais qu'il contraint également les employés à s'interroger sur la moindre de leurs décisions et le moindre de leurs commentaires. Le respect de la vision de l'entreprise finit par coûter trop cher en termes d'autonomie et de liberté individuelles. » [469]

C'est d'ailleurs ce qui explique qu'en matière de surveillance vidéo, les tribunaux mettent beaucoup d'importance sur la manière dont les caméras sont placées, vers qui elles sont dirigées et les activités menées par les employés lorsqu'ils sont surveillés[470].

---

[466] À titre d'illustration en matière de surveillance vidéo, voir : *Liberty Smelting Works (1962) Ltd. et Syndicat international des travailleurs unis de l'automobile, de l'aéronautique, de l'astronautique et des instruments aratoires d'Amérique (T.U.A.), local 1470*, préc., note 383; *Association des techniciennes et techniciens en diététique du Québec et Centre hospitalier Côte-des-Neiges*, préc., note 385, 1028 et 1029; *Vifan Canada inc. et Syndicat des travailleuses et travailleurs de Vifan Canada inc. (CSN)*, préc., note 243, par. 31; et COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2004-279, préc., note 425. En matière de fouille, voir *Syndicat démocratique des employés de commerce Saguenay-Lac-St-Jean et Potvin & Bouchard inc.*, préc., note 217.

[467] Par analogie avec les propos de l'arbitre Me Carol Jobin en matière de surveillance vidéo dans l'affaire *Syndicat des cols bleus regroupés de Montréal, section locale 301 et Montréal (Ville de) (arrondissement Côte-St-Luc—Hampstead—Montréal-Ouest)*, préc., note 378, 1081: « Ce qui est interdit parce qu'il s'agit d'une condition de travail déraisonnable, c'est que ces caméras de surveillance soient constamment braquées sur des individus, épiant ainsi systématiquement leurs faits et gestes. Il s'agit alors d'une forme de harcèlement au même titre que si un contremaître s'installait en permanence auprès d'un salarié pour le surveiller pendant toute la durée de son travail. La mesure prise par l'employeur doit donc être exercée et utilisée de manière seulement à atteindre le but légitime poursuivi, et être limitée aux lieux ou activités dans lesquelles l'entreprise subit un réel problème. »

[468] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2004-279, préc., note 425.

[469] *Id.*, p. 4.

[470] À titre d'illustration, voir : *Association des techniciennes et techniciens en diététique du Québec et Centre hospitalier Côte-des-Neiges*, préc., note 385, 1029; *Société des alcools du Québec et Syndicat des travailleuses*

Par ailleurs, une mesure ciblée à un échantillon d'employés peut laisser croire que les employés visés sont soupçonnés d'activités illégales ou interdites, ou encore d'un manquement à leurs obligations contractuelles et risque plus facilement d'être considéré déraisonnable. Dans ce contexte, les employés pourraient plus facilement contester la mesure pour le motif qu'elle est exercée de manière discrétionnaire ou discriminatoire et qu'elle constitue une mesure disproportionnelle[471]. À moins que des faits particuliers justifient ou rendent nécessaire cette surveillance ciblée à un employé ou un groupe d'employé en particulier[472], il est donc recommandé de soumettre tous les employés à la surveillance.

Sous réserve des autres critères, une pratique de surveillance ou de contrôle faite de façon spontanée[473], ou encore ponctuelle et limitée dans le temps[474], est généralement considérée raisonnable et proportionnelle à l'objectif recherché. Si elle est effectuée épisodiquement à l'égard de certains employés (échantillonnage), il est recommandé que la sélection des employés se fasse au hasard[475].

---

et travailleurs de la Société des alcools du Québec (SCFP), section locale 3535T, préc., note 385, par. 60-63; et *Syndicat des cols bleus regroupés de Montréal, section locale 301 et Montréal (Ville de) (arrondissement Côte-St-Luc—Hampstead—Montréal-Ouest)*, préc., note 385, 1077-1081; *Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleuses et travailleurs du Canada et BMW Canbec*, préc., note 215, par. 42; *Vifan Canada inc. et Syndicat des travailleuses et travailleurs de Vifan Canada inc. (CSN)*, préc., note 243, par. 28 à 39.

[471] Par analogie avec les principes établis en matière de fouille au travail et illustrés dans l'affaire *Re Amalgamated Electric Corp. Ltd. (Markham) and International Brotherhood of Electrical Workers, Local 1590* (1974), 6 L.A.C. (2d) 28 (Ont. Arbitration Board); *Re University Hospital and London & District Service Worker's Union, Local 220* (1981), 28 L.A.C. (2d) 294 (Ont. Arbitration Board). Voir également B. TURMEL, préc., note 404, à la page 66.

[472] Notamment si l'employeur entretient des doutes sérieux à l'égard d'un employé ou d'un groupe d'employés en particulier. Voir à titre d'illustration en matière de surveillance vidéo l'affaire *Poulies Maska inc. et Syndicat des employés de Poulies Maska inc.*, préc., note 243.

[473] À titre d'illustration en matière de fouille des employés, voir : *Syndicat des employés des Aciers Atlas (C.S.N.) et Aciers Atlas, Une Division de Rio Algom Ltd.*, D.T.E. 83T-478, AZ-83141237 (T.A.); *Re Lornex Mining Corp. and United Steelworkers, Local 7619* (1983), 14 L.A.C. (3d) 169 (B.C. Arbitration Board), 183.

[474] À titre d'illustration en matière de surveillance vidéo, voir : *Syndicat national des employés de garage du Québec inc. et Sovea Auto ltée*, préc., note 402, p. 23; *Syndicat des employés de l'aluminerie de Baie-Comeau (CSN) et Alcoa ltée (Aluminerie de Baie-Comeau)*, préc., note 402, p. 51; *Syndicat des employées et employés de la Société des casinos du Québec, section unité générale (CSN) et Société des casinos du Québec*, préc., note 402, p. 54-55.

[475] Pour des illustrations jurisprudentielles dans lesquelles le mode de sélection en matière de fouille est fait au hasard, voir : *Syndicat des employés des Aciers Atlas (C.S.N.) et Aciers Atlas, Une Division de Rio Algom Ltd.*,

Le caractère minimal de l'atteinte est également apprécié au regard du nombre de personnes au sein de l'entreprise ayant accès aux résultats de la surveillance. Plus le nombre de personnes ayant accès aux images, rapports, films, ou tout autre renseignement obtenu dans le cadre de la surveillance est élevé, plus l'atteinte aux droits des personnes assujetties est élevée et plus la mesure risque d'être considérée disproportionnée par rapport à l'objectif poursuivi[476].

Finalement, si les employés ont préalablement été informés de l'existence de la mesure exercée par l'employé, ou encore ont consenti à l'implantation de cette mesure au sein de l'entreprise, l'atteinte aux droits des employés sera moindre que dans la situation inverse, et l'employeur aura plus de facilité à établir la proportionnalité de l'atteinte[477]. En effet, tel que vu précédemment, l'information donnée aux employés de même que l'obtention de leur consentement à l'égard d'une mesure de surveillance ou de contrôle a pour effet de réduire leur niveau d'expectative de vie privée à l'égard de l'activité surveillée ou contrôlée. Nous traiterons plus en détail de la manière d'informer les employés et d'obtenir leur consentement dans la section suivante. Pour l'instant, nous nous limitons à recommander à l'employeur d'adopter une politique de surveillance écrite, de tenir des séances d'information ou de distribuer des pamphlets ou des avis d'information quant à l'existence de la mesure de surveillance, et si possible d'obtenir leur consentement à cet égard.

À la lumière de ce qui précède, les employeurs ont avantage à être diligents lorsqu'ils

---

préc., note 473; *Philips Électronique Ltée et Syndicat des travailleurs unis de l'électrocité, radio et machinerie du Canada, section locale 565*, [1991] T.A. 139, D.T.E. 91T-294; *Re Johnson Matthey & Mallory Ltd. and Precious Metal Workers Union, Federal Local 24739* (1975), 10 L.A.C. (2d) 354 (Ont. Arbitration Board) et *Re Lornex Mining Corp. and United Steelworkers, Local 7619*, préc., note 473.

[476] Par analogie avec les principes établis en matière de surveillance vidéo et illustrés dans l'affaire *Poulies Maska inc. et Syndicat des employés de Poulies Maska inc.*, préc., note 243, p. 9; et *Société des alcools du Québec et Syndicat des travailleuses et travailleurs de la Société des alcools du Québec (SCFP), section locale 3535T*, préc., note 385.

[477] *Poulies Maska inc. et Syndicat des employés de Poulies Maska inc.*, préc., note 243. En l'espèce, l'employeur avait tenu des séances d'informations auprès de ses employés et leur avait expliqué au travail que désormais, il y avait des caméras sur place et que les employés pouvaient être filmés.

mettent en place une surveillance des employés et à réfléchir à la manière dont celle-ci sera exécutée. Cela concerne en premier lieu l'étendue de la surveillance, à savoir (i) qui sera assujetti et la manière dont se fera la sélection des employés; (ii) à quel moment les employés seront surveillés et dans quel contexte; (iii) quelle(s) activité(s) sera(ont) surveillée(s) ; et (iv) qui aura accès aux résultats de la surveillance, et en deuxième lieu les mesures prises par l'employeur en parallèle à l'implantation de la surveillance, à savoir (i) le niveau de transparence de la surveillance ; et (ii) l'acceptation de la surveillance par les employés comme condition de travail.

3.1.3.2.2. L'APPLICATION EN MATIÈRE DE SURVEILLANCE DE L'UTILISATION D'INTERNET

En matière de surveillance de l'utilisation d'Internet, nous avons vu, dans le cadre du premier chapitre[478], les différents types de surveillance pouvant être exercés par un employeur au niveau de l'utilisation d'Internet. L'employeur peut notamment exercer une surveillance limitée à un seul employé, ou encore l'étendre à l'ensemble de ses employés. L'employeur peut exercer une surveillance ponctuelle, limitée dans le temps, ou encore de manière continue et permanente. L'employeur peut également limiter la surveillance à une ou plusieurs applications Internet.

Dépendamment du type de surveillance choisi par l'employeur, la vie privée et la dignité des employés se verront plus ou moins brimées. L'atteinte à la vie privée et à la dignité des employés sera plus importante si la surveillance est exercée de manière permanente et étendue à l'ensemble des applications Internet, par rapport à une surveillance limitée à une utilisation d'Internet bien précise et durant une courte période prédéterminée.

Dans l'affaire *Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada*[479], l'arbitre avait d'ailleurs considéré le fait que la surveillance de

---

[478] *Supra*, p. 38.

[479] Préc., note 136.

l'utilisation d'Internet n'était pas exercée de manière continue ou systématique, afin de conclure qu'il n'était pas abusif ni illégal de la part de l'employeur de fouiller dans le disque dur de l'employé pour recouvrer l'historique des sites Internet consultés durant les heures de travail[480]. De plus, en l'espèce, les employés du musée avaient reçu plusieurs avis verbaux et notes de services leur indiquant que les outils informatiques et l'accès Internet devaient être utilisés uniquement pour le travail et pour les fins du musée, et l'employé en question s'était fait avertir à plusieurs reprises de suivre ces consignes.

Par conséquent, l'employeur doit s'assurer, lorsqu'il délimite l'étendue dans le temps et dans l'espace de la surveillance, que cette étendue est justifiée eu égard aux objectifs légitimes et importants qu'il a préalablement identifiés. Une fois les objectifs identifiés à la lumière des risques et incidents subis par l'employeur dans le cadre de l'utilisation d'Internet, l'employeur doit s'assurer que la surveillance telle qu'il entend l'exercer, est réellement nécessaire et efficace pour atteindre le ou les objectif, et est menée de la manière la moins intrusive possible. Cette analyse doit se faire à la lumière de chacun des aspects suivants :

- l'étendue des activités Internet sujettes à la surveillance (courrier électronique, navigation, blogs, messagerie instantanée, téléchargement de fichiers) ;

- l'étendue dans le temps de la surveillance (ponctuelle, limitée à certaines heures de la journée, i.e. uniquement durant les heures de travail, ou exercée de manière permanente) ;

- l'étendue des employés soumis à la surveillance (un seul, quelques-uns, tous) ;

- Les informations données aux employés quant à la surveillance et les consentements obtenus quant à l'exercice de cette surveillance ;

---

[480] *Id.*, 481.

- les mesures prises pour assurer la confidentialité des informations obtenues (accès restreint aux résultats de la surveillance, mise sous-clé des résultats) ;

- autres mesures (i.e. mise en place d'un système de courrier électronique distinct pour les messages personnels qui, lui, n'est pas soumis à la surveillance)[481].

Chaque situation est un cas d'espèce. Ce qu'il faut en retenir, c'est que l'exercice de la surveillance doit répondre au critère de proportionnalité sous tous ses angles. Si l'employeur suspecte un problème sérieux au niveau de l'utilisation du courriel, il n'est pas nécessaire de surveiller également la navigation sur Internet. Si l'employeur a remarqué une importante baisse de productivité au niveau du travail d'un seul de ses employés, il n'est pas nécessaire de soumettre tous ses employés à l'exercice de la surveillance.

La plupart des logiciels de surveillance vendus sur le marché offrent une grande variété d'options dans le cadre de l'exercice de la surveillance. Il faut donc que l'employeur soit vigilant lorsqu'il implante le logiciel au sein de son entreprise, de manière à n'utiliser que les options qui lui sont absolument nécessaires et efficaces pour répondre aux objectifs et qui offrent une atteinte minimale tant à la vie privée qu'à la dignité de l'employé.

Par ailleurs, même si la surveillance de l'utilisation d'Internet est exercée de la manière la moins intrusive possible pour atteindre les fins recherchées, il n'est pas toujours nécessaire de recourir à ce type de surveillance. En effet, il peut y avoir des moyens encore moins envahissants que la surveillance de l'utilisation d'Internet pour atteindre les fins recherchées. L'employeur ne doit donc pas uniquement s'assurer qu'il exerce la surveillance électronique la moins envahissante possible ; il doit également s'assurer qu'il n'y a pas d'autres mesures moins envahissantes que la

---

[481] K. DELWAIDE, « La protection de la vie privée et les nouvelles technologies : l'accès au courrier électronique des employés par un employeur », préc., note 242, à la page 661.

surveillance en tant que telle[482].

À cet égard, nous reprenons les principes énoncés par le Commissaire à la protection de la vie privée du Canada en matière de prévention du harcèlement sexuel au travail :

> « La prévention du harcèlement en milieu de travail représente certes un objectif important, mais la meilleure façon d'atteindre celui-ci reste la formation et la sensibilisation des employés et l'instauration de politiques explicites contre le harcèlement et des mesures de redressement appropriées lorsque des problèmes de harcèlement sont déclarés ou qu'on a des motifs raisonnables de soupçonner le harcèlement, plutôt que le déni à tous les employés de leurs droits en matière de protection de leurs renseignements personnels. »[483]

Le principe de la nécessité de l'atteinte est notamment illustré en matière de surveillance des comptes de courrier électronique d'employés dans une décision du Commissaire à la protection de la vie privée du Canada suite à une plainte portée contre la Commission de l'immigration et du statut de réfugié (CISR)[484].

En l'espèce, l'employé avait eu des échanges par courrier électronique avec le syndicat et lui avait fourni copie des évaluations du rendement de certains employés de la Commission. Or, l'extrait de ces échanges électroniques n'était pas nécessaire pour découvrir la faute de l'employé, compte tenu que la Commission était déjà au courant des actes de l'employée et des échanges intervenus avec le syndicat. Dans ce contexte, le Commissaire à la protection de la vie privée du Canada s'est exprimé comme suit : « Il n'était pas nécessaire que la CISR extraie les messages électroniques échangés afin de déterminer si des mesures disciplinaires devaient être prises à l'endroit de

---

[482] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2004-279, préc., note 425, p. 4.

[483] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Fiche d'information - La protection des renseignements personnels au travail*, 19 février 2004, en ligne : http://www.privcom.gc.ca/fs-fi/02_05_d_17_f.asp.

[484] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Conclusions en vertu de la *Loi sur la protection des renseignements personnels, Surveillance indue des comptes de courrier électronique d'employés* (2001-2002), en ligne : http://www.priv.gc.ca/cf-dc/pa/2001-02/pa_200102_05_f.cfm.

l'employée. »[485]

Finalement, afin que l'atteinte soit minimale, il est nécessaire que l'employeur respecte les obligations qui lui sont applicables en vertu des lois sur la protection des renseignements personnels[486]. Ces lois, qui visent à protéger la vie privée des individus, imposent diverses obligations aux personnes qui traitent des renseignements personnels, que ce soit au niveau de la collecte, la conservation, l'usage et la divulgation de renseignements personnels. La surveillance de l'utilisation d'Internet au travail tombe donc sous le coup de cette loi et les employeurs doivent respecter les obligations qui en découlent.

Dans la prochaine section, nous exposerons les diverses obligations qui incombent à l'employeur dans le cadre de la mise en place d'une surveillance de l'utilisation d'Internet au travail, une fois que les critères de rationalité et de proportionnalité sont respectés. Nous verrons par ailleurs que le respect de ces obligations peut avoir un effet très favorable pour l'employeur dans l'analyse du critère de proportionnalité.

3.2. Les obligations préalables à la surveillance de l'utilisation d'Internet au travail

L'analyse des critères de rationalité et de proportionnalité ajoutée à celle de l'expectative raisonnable de vie privée des employés à l'égard des activités Internet permet aux employeurs de déterminer de manière approximative à quel niveau se situent les droits de leurs employés par rapport à leur pouvoir de direction et de contrôle. Cette délimitation est nécessaire pour pouvoir établir approximativement la manière dont ils devront mener la surveillance et les obligations qui leur incombent à cet égard.

Dans certains cas, l'analyse de ces éléments exigera de l'employeur que les personnes

---

[485] *Id.*, p. 1.

[486] Pour un énoncé général des obligations applicables, voir COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Fiche d'information - La protection des renseignements personnels au travail*, préc., note 483.

surveillées soient préalablement informées de la surveillance et aient donné leur consentement à cet égard. Il s'agira de situations où l'expectative raisonnable de vie privée des employés est plus élevée, ou encore lorsque les objectifs poursuivis par l'employeur bien que respectant le critère de rationalité, se situent à un niveau moindre quant à leur légitimité et leur importance. Le cas échéant, ces obligations sont nécessaires pour que l'atteinte à la vie privée ou à des conditions de travail justes et raisonnables soit minimale et que le critère de proportionnalité soit respecté. Le respect des obligations d'information et de consentement ont pour effet de réduire l'expectative de vie privée des personnes surveillées et ainsi de rétablir une balance entre les différents intérêts en jeu.

Dans d'autres cas, les intérêts invoqués par l'employeur seront tellement légitimes et importants, ou encore la nature de l'emploi ou de l'entreprise sera telle, que l'employeur pourra exercer une surveillance de l'utilisation d'Internet sans être soumis aux obligations d'information et de consentement. Le cas échéant, l'expectative raisonnable de vie privée de l'employé est suffisamment minime ou prend moins de poids dans la balance des intérêts par rapport aux intérêts de l'employeur, et le respect des obligations d'information et de consentement n'est pas requis.

Nous exposerons maintenant en détails en quoi consiste l'obligation d'informer les employés, d'obtenir leur consentement à l'égard de la surveillance et d'adopter une politique de surveillance, ces trois obligations potentielles étant les plus importantes et les plus complexes pour un employeur qui désire mettre en place une surveillance de l'utilisation d'Internet au travail. À cet égard, nous fournirons aux employeurs des lignes directrices générales qui leur permettront de se poser les bonnes questions afin de déterminer s'ils doivent ou non remplir ces obligations.

3.2.1. Les obligations d'information et de consentement

Il est recommandé que l'employeur informe ses employés de l'exercice de la surveillance et obtienne leur consentement à cet égard, et ce, pour deux motifs : (i) afin de réduire l'expectative raisonnable de vie privée des employés dans le cadre de

leur utilisation d'Internet au travail; et (ii) afin de respecter les obligations légales découlant de la protection des renseignements personnels.

3.2.1.1. Le champ d'application des obligations d'information et de consentement

3.2.1.1.1. LA RÉDUCTION DE L'EXPECTATIVE RAISONNABLE DE VIE PRIVÉE

Réduire l'expectative raisonnable de vie privée de l'employé dans le cadre de l'utilisation d'Internet au travail permet en quelque sorte de renforcer le droit de surveillance de l'employeur à l'égard des activités Internet menées par ses employés. À ce titre, et sous réserve des obligations qui incombent à l'employeur en matière de protection des renseignements personnels, l'obligation d'information et de consentement ne constituent pas des obligations strictes pour l'employeur qui entend surveiller l'utilisation d'Internet au travail. Tel que vu précédemment[487], la connaissance et le consentement de l'employé font plutôt partie des facteurs qui entrent en ligne de compte lors de l'analyse de l'expectative de vie privée de l'employé et de l'appréciation de la proportionnalité de l'atteinte.

Néanmoins, dans certaines circonstances, le respect de ces deux exigences jouera un rôle suffisamment déterminant pour être considéré comme une quasi-obligation pour l'employeur. Il s'agira notamment des situations dans lesquelles l'expectative de vie privée de l'employé dans le cadre de ses activités Internet au travail est trop élevée par rapport aux intérêts de l'employeur, lorsque les intérêts soulevés par l'employeur touchent des intérêts purement économiques (ex. productivité) sans être fondés sur la survenance de réels problèmes au sein de l'entreprise, ou encore lorsque l'employeur cherche à prévenir un risque plutôt qu'enrayer un problème sérieux dont il est victime.

À cet égard, il faut appliquer par analogie les principes établis en matière de fouille

---

[487] *Supra*, p. 80 et suiv.

des employés, plus particulièrement au niveau de la reconnaissance de l'atteinte à la vie privée comme condition d'emploi. En matière de fouille, un employeur a le droit de fouiller ses employés si ceux-ci ont préalablement reconnu (explicitement ou implicitement) la fouille comme une de leurs conditions d'emploi[488]. Ils doivent donc être au courant et y avoir consenti d'une certaine manière.

Nous n'affirmerons pas ici que, à l'instar du droit de fouille, la reconnaissance implicite ou explicite de la mesure de l'employeur est une condition préalable à son droit de surveillance. En effet, en matière de fouille, à l'exception du casier personnel, l'objet fouillé appartient généralement à l'employé, alors qu'en matière de surveillance de l'utilisation d'Internet, l'ordinateur appartient à l'employeur, d'autant plus qu'un casier est généralement fourni à l'employé pour y entreposer ses effets personnels alors que l'ordinateur est fourni pour lui permettre d'exercer ses fonctions de travail[489]. Le niveau d'expectative de vie privé en matière de fouille étant plus élevé dans ce contexte, les critères applicables à l'employeur doivent en principe être plus sévères qu'à l'égard de la surveillance de l'utilisation d'Internet au travail.

Il est plutôt utile de s'inspirer des principes établis en matière de fouille pour définir la manière d'informer les employés et d'obtenir leur consentement quant à la surveillance de l'utilisation d'Internet, et ce dans les cas suivants : (i) lorsque le niveau d'expectative de vie privée de l'employé est très élevé, faisant en sorte que la connaissance et le consentement de l'employé à la surveillance deviennent une « quasi-obligation » ; et (ii) lorsque l'employeur veut mettre toutes les chances de son côté pour renforcer sont droit de surveillance de l'utilisation d'Internet au travail.

Ainsi, le droit de surveillance de l'employeur sera renforcé s'il existe une clause

---

[488] *Entreprises Cara Ltée et Association internationale des machinistes et des travailleurs de l'aéroastronautique, loge 987*, préc., note 404, 13; *Syndicat des travailleurs de l'énergie et de la chimie, section locale 107* c. *Laurin*, préc., note 272, p. 6; *Corp. Outils Québec et Syndicat indépendant des salariés de Outils Québec*, préc., note 272, 654; *Re United Automobile Workers, local 444 and Chrysler Corporation of Canada Limited* (1961), 11 L.A.C. 152 (Ont. Arbitration Board), 158-162; et *Re Amalgamated Electric Corp. Ltd. (Markham) and International Brotherhood of Electrical Workers, Local 1590*, préc., note 471, 31-33.

[489] *McLaren* v. *Microsoft Corp.*, préc. note 141, p. 4.

contractuelle à cet effet dans le contrat d'emploi, dans le formulaire d'embauche que les employés signent ou dans la convention collective négociée par le syndicat[490], si une politique de surveillance a été adoptée à cet effet[491], ou encore si une pratique passée de surveillance de l'utilisation d'Internet est bien établie, connue et acceptée de tous les employés[492]. L'idée est que tous les employés soient au courant de cette surveillance et la reconnaissent comme faisant partie de leurs conditions d'emploi[493].

3.2.1.1.2. LE RESPECT DES LOIS SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Les lois fédérales et québécoises sur la protection des renseignements personnels imposent une obligation d'information et de consentement à quiconque recueille, utilise ou communique des renseignements personnels sur un individu[494]. Par conséquent, si l'employeur collecte des renseignements personnels sur ses employés ou sur des tiers lors de la surveillance de l'utilisation d'Internet, il devient automatiquement soumis à ces obligations d'information et de consentement.

Jusqu'à aujourd'hui, aucune décision arbitrale ou judiciaire québécoise n'a traité de ces obligations légales dans le cadre de la surveillance de l'utilisation d'Internet au travail. Néanmoins, le Commissariat à la protection de la vie privée du Canada a

---

[490] À titre d'illustration en matière de fouille au travail, voir : *Canapar Ltée et Fraternité nationale des charpentiers-menuisiers, forestiers, travailleurs d'usines*, préc., note 404; et *Re United Automobile Workers, local 444 and Chrysler Corporation of Canada Limited*, préc., note 488.

[491] À l'égard des politiques de surveillance, nous référons le lecteur à la section 3.3, *infra*, p. 177.

[492] À titre d'illustration en matière de fouille, voir : *Syndicat des employés des Aciers Atlas (C.S.N.) et Aciers Atlas, Une Division de Rio Algom Ltd.*, préc., note 473; *Syndicat international des travailleurs de la boulangerie, confiserie et du tabac, section locale 476 F.A.T.-C.I.O.-C.T.C. et Walter M. Lowney Co.*, préc., note 272; *Entreprises Cara Ltée et Association internationale des machinistes et des travailleurs de l'aéroastronautique, loge 987*, préc., note 404; *Canapar Ltée et Fraternité nationale des charpentiers-menuisiers, forestiers, travailleurs d'usines*, préc., note 404; *Philips Électronique Ltée et Syndicat des travailleurs unis de l'électrocité, radio et machinerie du Canada, section locale 565*, préc., note 475; *Syndicat des travailleurs de l'énergie et de la chimie, section locale 107* c. *Laurin*, préc., note 272; et *Re United Electrical Workers, local 504 and Canadian Westinghouse Co. Ltd.* (1964), 15 L.A.C. 348 (Ont. Arbitration Board).

[493] L. BERNIER, L. GRANOSIK et J.-F. PEDNAULT, préc., note 270, p. 21-35 à 21-36; et B. TURMEL, préc., note 404, aux pages 58 et 59;.

[494] Loi sur l'accès, art. 65; Loi sur le secteur privé, art. 8; L.p.r.p., art. 5(2); et L.p.r.p.d.é., art. 5(1) et annexe 1, principes 4.2.1, 4.2.3 et 4.2.5.

rendu plusieurs conclusions et avis en la matière[495], et les obligations d'information et de consentement découlant des lois sur la protection des renseignements personnels ont été considérées à plusieurs reprises en matière de surveillance vidéo[496], d'écoute électronique des employés[497] et de collecte de renseignements personnels sur les employés au moyen de GPS[498]. Ces décisions et avis illustrent l'importance d'aviser clairement les personnes à l'égard des renseignements personnels qui seront collectés ou utilisés à leur égard.

Nous référons le lecteur à la section 2.2.1.2.2.4.3.[499] quant aux renseignements personnels pouvant être collectés dans le cadre de la surveillance et qui entraînent, le cas échéant, la soumission de l'employeur aux obligations d'information et de consentement prévues dans ces lois.

3.2.1.2. L'étendue des obligations

3.2.1.2.1. L'OBLIGATION D'INFORMATION

Les informations que l'employeur doit donner à son ou ses employés soumis à la

---

[495] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Surveillance indue des comptes de courrier électronique d'employés*, préc., note 484; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Fiche d'information - La protection des renseignements personnels au travail*, préc., note 483; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Trouver le bon équilibre en ce qui concerne la protection de la vie privée au travail*, Allocution prononcée par Jennifer Stoddart, Toronto, 30 novembre 2006, en ligne : http://www.privcom.gc.ca/speech/2006/sp-d_061130_f.asp; et COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Conclusions en vertu de la *Loi sur la protection des renseignements personnels, Surveillance des courriels d'un employé se révèle appropriée* (2007-2008), en ligne http://www.priv.gc.ca/cf-dc/pa/2007-08/pa_200708_05_f.cfm.

[496] *Eastmond* c. *Canadian Pacific Railway*, préc., note 363. Voir également COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumés de conclusions d'enquêtes en vertu de la LPRPDÉ n° 2004-264, préc., note 425; n° 2004-273, préc., note 425; et n° 2005-290, préc., note 425.

[497] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2007-387 – *Une station de télévision enregistre indûment la conversation téléphonique d'un employé,* en ligne : http://www.priv.gc.ca/cf-dc/2007/387_20061204_f.cfm.

[498] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2006-351 – *Examen de l'utilisation des renseignements personnels recueillis au moyen d'un système mondial de localisation*, en ligne : http://www.priv.gc.ca/cf-dc/2006/351_20061109_f.cfm.

[499] *Supra*, p. 106.

surveillance de l'utilisation d'Internet sont les suivantes[500] : (i) la liste des activités Internet qui seront soumises à la surveillance ; (ii) les objectifs recherchés par la mise en place de surveillance, les risques que l'employeur cherche à enrayer; (ii) une description de la manière dont la surveillance sera exercée ; (iii) l'étendue de cette surveillance (continue, ponctuelle, sporadique, heures de surveillance, etc.) ; (iv) la liste des renseignements personnels qui seront recueillis, utilisés et communiqués dans le cadre de la surveillance ; (v) l'utilisation qui en sera faite ainsi que les catégories de personnes qui y auront accès au sein de l'organisation ; et (vi) l'endroit où sera détenu le dossier de l'employé ainsi que ses droits d'accès et de rectification.

Bien que l'employeur ne soit pas toujours en mesure d'identifier à l'avance les renseignements de nature personnelle qui seront collectés par le biais de la surveillance, il peut néanmoins prévoir, selon le type de surveillance exercé, ceux qui sont susceptibles d'être collectés. Si par exemple l'employeur surveille le courrier électronique de ses employés, il pourra prévoir que les messages à caractère personnel feront l'objet d'une surveillance. Si par ailleurs l'employeur surveille l'historique des sites web visités, il pourra prévoir qu'il collectera également tout l'historique des sites web visités à des fins personnelles.

Les fins auxquelles les renseignements personnels sont destinés doivent par ailleurs répondre au critère de rationalité. Tel qu'exposé précédemment, les diverses lois sur la protection des renseignements personnels prévoient des critères similaires aux chartes afin de restreindre le droit à la vie privée[501]. Ces fins doivent donc répondre aux principes énoncés dans la section 3.1.3.1.[502]

La manière dont cette information doit être fournie par l'organisation n'est pas

---

[500] En matière de vie privée, plus l'employé aura reçu de l'information quant aux activités Internet surveillées au travail, plus son expectative de vie privée pourra en être réduite. À cet égard, l'employeur doit suivre les principes en matière de protection des renseignements personnels. Voir à cet effet Loi sur l'accès, art. 65; Loi sur le secteur privé, art. 8; L.p.r.p., art. 5(2); et L.p.r.p.d.é., art. 5(1) et annexe 1, principes 4.2.1, 4.2.3 et 4.2.5.

[501] *Supra*, p. 127.

[502] *Supra*, p. 132.

précisée dans la législation. Les informations peuvent être données soit verbalement, soit par écrit, que ce soit sous forme de politique, de directive, ou sous toute autre forme de documentation, l'important étant que l'information soit fournie de manière compréhensible et facilement accessible aux employés ou aux tiers[503]. À ce titre, il est fortement recommandé aux employeurs d'adopter une politique de surveillance qui sera distribuée ou autrement portée à la connaissance de tous les employés[504]. Il est également recommandé d'afficher des avis à plusieurs endroits, ou encore de faire des rappels écrits régulièrement[505]. D'ailleurs, dans l'une de ses conclusions, le Commissariat à la protection de la vie privée a conclu que l'employeur avait fait preuve d'équité et de transparence en informant ses employés de ses pratiques de surveillance par le biais de l'avis électronique et en versant à son site intranet les directives s'appliquant à son réseau électronique[506]. En l'espèce, l'employé se plaignait de l'obligation qu'il avait d'acquiescer à un avis qui s'affichait à son écran d'ordinateur chaque fois qu'il souhaitait accéder au système informatique de l'organisme, sous peine de s'en voir refuser l'accès.

Dans l'affaire *Blais et La Société des Loteries Vidéos du Québec Inc.*[507], l'employeur avait effectué de la formation auprès de ses employés quant aux politiques et directives relatives à l'utilisation d'Internet au travail, et avait distribué des dépliants quant aux règles d'utilisation du courrier électronique au travail, lesquels contenaient des clauses explicites à l'effet que l'entreprise pouvait avoir à accéder au contenu des

---

[503] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Guide à l'intention des entreprises et des organisations – Protection des renseignements personnels : vos responsabilités*, mars 2004, en ligne : http://www.priv.gc.ca/information/guide_f.pdf, p. 19.

[504] À l'égard des politiques de surveillance, voir *infra*, section 3.3, p. 177.

[505] Par analogie avec les propos énoncés dans *Entreprises Cara Ltée et Association internationale des machinistes et des travailleurs de l'aéroastronautique, loge 987*, préc., note 404, 14. En l'espèce, tous les envoyés avaient reçu copie du règlement et plusieurs avis avaient été affichés à plusieurs endroits. Plusieurs rappels écrits avaient été faits par l'employeur. Dans ce contexte, le tribunal a conclu que l'employé devait savoir que la vérification de ses effets personnels faisait partie de ses conditions d'emploi.

[506] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Conclusions en vertu de la Loi sur la protection des renseignements personnels, Le gouvernement a le droit de surveiller l'utilisation de ses systèmes de courrier électronique* (2005-2006), en ligne : http://www.privcom.gc.ca/cf-dc/pa/2005-06/pa_200506_06_f.cfm.

[507] Préc., note 136.

messages électroniques et que les employés ne pouvaient prétendre au caractère privé de leurs messages électroniques.

La Cour a notamment considéré ces faits pour conclure qu'en aucun moment l'employé ne pouvait prétendre au caractère privé de ses échanges. Dans cette affaire, si l'employeur n'avait pas eu de politique de surveillance ou que les employés n'en avaient pas été informés, peut-être la Commission aurait-elle conclu autrement. Le cas échéant, l'employeur n'aurait pu produire en preuve tous les courriels tirés de la boîte de courrier électronique du plaignant.

Par ailleurs, dans l'affaire *Syndicat des professionnelles et professionnels des affaires sociales du Québec (C.S.N.) et Institut de réadaptation en déficience physique de Québec*[508], l'arbitre Me René Turcotte a conclu que l'employeur n'avait pas violé les droits des plaignants en vérifiant le contenu de leurs ordinateurs de travail, compte tenu notamment de l'existence d'une réglementation interne quant à l'accès au contenu de ces ordinateurs et du fait que cette réglementation avait été faite dans le respect des règles et avec la plus grande prudence[509].

À la lumière des décisions précitées, il apparaît que l'employeur a tout intérêt à informer ses employés de l'existence de la surveillance, de même que des motifs et de l'étendue d'une telle surveillance, que ce soit en vertu des obligations légales auxquelles il est assujetti, ou tout simplement pour renforcer son droit de surveillance.

3.2.1.2.2. L'OBLIGATION DE CONSENTEMENT

Une fois que les employés sont bien informés de l'existence et de l'étendue de la surveillance, l'employeur doit s'assurer d'obtenir leur consentement. Les employés doivent consentir au fait que l'employeur portera atteinte à leur vie privée par le biais de la surveillance, collectera des renseignements personnels les concernant pour des

---

[508] Préc., note 154.

[509] *Id.*, par. 293.

fins déterminées, et confinera les résultats dans un dossier afin de les utiliser pour ces fins.

Le consentement ne peut être obtenu de n'importe quelle façon et doit respecter un certain nombre de conditions pour être reconnu valide au sens de ces lois. Plus particulièrement, le consentement doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Un consentement qui ne répond pas à ces exigences sera, en vertu de la loi, sans effet[510].

Pour qu'un consentement soit manifeste, il doit être clair et non équivoque. À cet égard, l'Annexe 1 de la L.p.r.p.d.é. indique que plus les renseignements personnels sont sensibles, plus l'organisation devra chercher à obtenir un consentement explicite :

> « **4.3.4** La forme du consentement que l'organisation cherche à obtenir peut varier selon les circonstances et la nature des renseignements. Pour déterminer la forme que prendra le consentement, les organisations doivent tenir compte de la sensibilité des renseignements. Si certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. Par exemple, les nom et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les nom et adresse des abonnés de certains périodiques spécialisés pourront l'être.
>
> (...)
>
> **4.3.6** La façon dont une organisation obtient le consentement peut varier selon les circonstances et la nature des renseignements recueillis. En général, l'organisation devrait chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles. Lorsque les renseignements sont moins sensibles, un consentement implicite serait normalement jugé suffisant. Le consentement peut également être donné par un représentant autorisé (détenteur d'une procuration, tuteur). »

Un consentement explicite peut être obtenu de différentes manières[511]. Il peut

---

[510] C.c.Q., art. 35 al. 2 et art. 37 ; Loi sur l'accès, art. 59; Loi sur le secteur privé, art. 13 et 14; L.p.r.p.d.é., art. 5 et annexe 1, principe 4.3. Voir également : *St-Amant* c. *Meubles Morigeau ltée,* [2006] R.J.Q. 1434 (C.S.), par. 22.

[511] Voir à cet égard les principes énoncés au principe 4.3.7 de l'annexe 1 de la L.p.r.p.d.é.

notamment être obtenu en personne, par téléphone, par la poste ou par courriel, et peut être obtenu tant verbalement que par écrit[512]. Il est néanmoins recommandé, pour une plus grande certitude, que l'employeur obtienne un consentement explicite écrit des personnes soumises à la surveillance[513].

Le consentement explicite pourra par ailleurs être établi par[514] : (i) une clause dans la formule d'embauche ou le contrat de travail signé par l'employé, ou encore dans la convention collective, indiquant que dans le cadre de son emploi, l'employé devra se soumettre à une surveillance quant à ses activités Internet; ou (ii) un règlement ou une politique de surveillance adoptée par l'employeur et approuvée par écrit par le syndicat ou les employés de la compagnie.

Dans certains circonstances, un consentement implicite pourra suffire, notamment lorsque l'expectative de vie privée est moindre ou que peu de renseignements sensibles seront collectés dans le cadre de la surveillance. Un consentement est implicite lorsque le comportement ou l'inaction de la personne intéressée permet raisonnablement de conclure au consentement.

À cet égard, par analogie avec les principes établis en matière de fouille des employés[515], une procédure de surveillance appliquée de manière suffisamment uniforme et constante depuis un certain nombre d'années, pourrait faire présumer un consentement implicite valide de la part des employés assujettis à cette surveillance. Le fait notamment que l'entreprise ait rappelé à plusieurs reprises à ses employés, par

---

[512] I. J. TURNBULL, préc., note 378, p. 65 : « Express consent is the straightforward agreement, given explicitly. This can be done orally or in written format. Such a form of consent is clear and does not require further interpretation. »

[513] Par analogie avec les principes énoncés dans *Allain* c. *Caisse populaire Laval-des-Rapides,* [2005] C.A.I 25 (C.A.I.), par. 18 : « La Commission est d'avis que ce consentement est manifeste puisqu'il est écrit (...) ».

[514] Par analogie, il est possible de se référer aux principes établis en matière de fouille : *Re United Automobile Workers, local 444 et Chrysler Corporation of Canada Limited*, préc., note 488, 159; et B. TURMEL, préc., note 404, à la page 58.

[515] *Entreprises Cara Ltée et Association internationale des machinistes et des travailleurs de l'aéroastronautique, loge 987*, préc., note 404, 13; *Syndicat des travailleurs de l'énergie et de la chimie, section locale 107* c. *Laurin*, préc., note 272, p. 6; et *Re United Electrical Workers, local 504 and Canadian Westinghouse Co. Ltd.*, préc., note 492.

le biais d'avis affichés à des endroits utiles ou remis à chacun des employés, qu'il pourrait être nécessaire de devoir surveiller leurs activités Internet ou de fouiller leur poste de travail informatique, pourrait entraîner une telle présomption, au même titre que si la surveillance a été mise en place depuis plusieurs années sans que le syndicat ou les employés n'aient jamais contesté ces pratiques. Par ailleurs, la politique de l'employeur doit être publiée de façon claire, être connue de façon certaine de tous les salariés et appliquée avec régularité et sans discrimination. En effet, une trop longue période entre la survenance des problèmes de l'employeur et l'application de la politique visant à l'enrayer pourra laisser croire à la caducité de la politique de l'employeur[516].

Tel que mentionné au deuxième chapitre[517], une telle pratique, si elle est bien établie au sein de l'entreprise, a pour effet de réduire le niveau d'expectative de vie privée de l'employé qui y est assujetti. Le cas échéant, l'existence d'une pratique de surveillance établie depuis longtemps au sein de l'entreprise a pour effet de réduire l'expectative de vie privée de manière suffisante pour pouvoir considérer que l'employé a implicitement consenti à la surveillance.

À l'égard du consentement implicite, le Commissariat à la protection de la vie privée du Canada a affirmé ce qui suit dans le cadre de conclusions d'une enquête portant sur l'utilisation des GPS pour surveiller les employés :

> « Lorsque l'on envisage de recourir au consentement implicite, on devrait également se référer au principe 4.3.5. Ce principe insiste sur la pertinence des attentes raisonnables de la personne et présente, en guise d'exemple, un scénario où le consentement d'une personne peut être implicite pour certaines fins, mais non pour d'autres. En résumé, lorsque le consentement est implicite, il ne devrait être implicite que pour les fins auxquelles un employé devrait raisonnablement s'attendre à ce que

---

[516] Par analogie avec les principes énoncés dans l'affaire *Syndicat international des travailleurs de la boulangerie, confiserie et du tabac, section locale 476 F.A.T.-C.I.O.-C.T.C. et Walter M. Lowney Co.*, préc., note 272, 676.

[517] *Supra*, p. 83.

les données soient utilisées. »[518]

Que le consentement soit explicite ou implicite, il doit être éclairé, c'est-à-dire que l'employé ou les tiers devront avoir été adéquatement informés, préalablement à l'émission du consentement, de tous les aspects liés à la surveillance, c'est-à-dire tous les renseignements qui découlent de l'obligation d'information exposée précédemment. Si l'obligation d'information telle qu'exposée précédemment est remplie par l'employeur, l'employé aura toutes les informations nécessaires pour émettre un consentement éclairé[519].

Quant au caractère libre du consentement, cette condition dépendra du moment où l'employé aura donné son consentement à l'exercice de la surveillance. En effet, cette condition s'apparente au caractère volontaire requis pour la validité d'une renonciation à la vie privée. Tel qu'exposé au deuxième chapitre[520], il apparaît difficile de conclure au caractère volontaire d'un consentement dans le contexte d'une relation de travail, compte tenu qu'un employé ne dispose normalement pas d'un pouvoir de négociation lors de l'émission du consentement. Par conséquent, il n'est pas recommandé d'obtenir le consentement au moment de l'embauche, et il est préférable que le consentement soit donné à la suite de négociations entre les parties ou, à tout le moins, après avoir laissé la chance à l'employé ou aux employés de donner leur avis ou commentaire quant à la mesure de surveillance.

Finalement, en matière de protection des renseignements personnels, le consentement doit être donné à des fins spécifiques, que ce soit pour la collecte, l'utilisation ou la communication des renseignements. En d'autres mots, le consentement doit encadrer la cueillette proposée et ne pas s'étendre au-delà de la période où s'accomplira l'objet du dossier. Par conséquent, il est préférable de ne pas faire signer des consentements

---

[518] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2006-351, préc., note 498.

[519] *Service d'aide au consommateur et Reliable (La), compagnie d'assurance-vie*, [1996] C.A.I. 406 (C.A.I.).

[520] *Supra*, p. 84.

vastes ou à caractère trop général.

Dans le cas où l'employeur ferait signer un formulaire de consentement général à ses employés, indiquant qu'ils consentent à la surveillance de l'utilisation d'Internet, l'employeur doit bien s'assurer que ce consentement couvre toutes les fins spécifiques recherchées par la surveillance, et qu'il n'a pas perdu sa valeur au fil du temps, à défaut de quoi il risque d'être déclaré invalide[521].

Par conséquent, le formulaire de consentement soumis par l'employeur dans le contexte d'une surveillance de l'utilisation d'Internet doit indiquer expressément le but visé par la surveillance, à défaut de quoi la personne concernée ne sera pas en mesure de prendre une décision éclairée et à des fins spécifiques[522]. Si par ailleurs le consentement demandé à l'employé n'est pas relié directement à l'objet du dossier, l'employeur devra donner un nouveau consentement pour une autre fin[523].

3.2.1.3. Les exceptions à l'obligation d'information et de consentement

3.2.1.3.1. GÉNÉRALITÉS

L'employeur n'a pas à informer ses employés ni à obtenir leur consentement à l'égard de la surveillance dans les situations suivantes : (i) si l'employé ne dispose d'aucune expectative de vie privée à l'égard des activités ou des communications Internet que l'employeur entend surveiller ; et (ii) si dans le cadre de la surveillance, l'employeur ne collecte pas de renseignements personnels sur ses employés.

La première situation est notamment illustrée dans l'affaire *R.* c. *Tremblay*[524] en

---

[521] Par analogie avec les principes énoncés dans l'affaire *Royal & Sun Alliance du Canada* c. *Québec (Ministère de la Sécurité publique)*, [2004] C.A.I. 345 (C.A.I.), 351.

[522] *Service d'aide au consommateur et Reliable (La), compagnie d'assurance-vie*, préc., note 519.

[523] *X. et Services aux marchands détaillants ltée*, [1996] C.A.I. 408, conf. par J.E. 2003-597, A.I.E. 2003AC-25, [2003] C.A.I. 667 (C.Q.).

[524] Préc., note 159. Voir également *Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada*, préc., note 136; et *Blais et La Société des Loteries Vidéos du Québec Inc.*, préc., note 136.

matière de saisie du disque dur d'un employé. En l'espèce, la Cour du Québec a conclu que la preuve n'avait pas été obtenue en violation de la vie privée de l'employé, compte tenu que dans les circonstances, ce dernier ne disposait d'aucune expectative raisonnable de vie privée. Pour en arriver à cette conclusion, la Cour a retenu les facteurs suivants : (i) la propriété de l'employeur quant à l'ordinateur et le bureau dans lequel travaillait le requérant ; (ii) le fait que le requérant était le 3^{e} plus haut gradé de son service ; (iii) la connaissance par l'employé de la directive de l'employeur visant l'usage qu'on doit faire des ordinateur ; et (iv) le fait que durant les heures de travail son bureau est ouvert et son ordinateur est ouvert en permanence.

Nous référons le lecteur à la section 2.2.1.2.2.[525] quant aux facteurs ayant pour effet de réduire la vie privée de l'employé. Il n'y a pas ici de formule clé, tout est du cas d'espèce. Toutefois, rappelons que cette absence d'expectative résultera généralement de la présence de plusieurs facteurs.

Par ailleurs, lorsque la surveillance de l'utilisation d'Internet risque de porter atteinte à la vie privée de l'employé ou d'être considérée comme une condition de travail injuste et déraisonnable, l'employeur pourra également faire abstraction des obligations d'information et de consentement dans les cas suivants : (i) si l'employé dispose d'une expectative de vie privée suffisamment faible ; et (ii) si la surveillance (incluant la collecte d'informations personnelles) effectuée au su et avec le consentement de l'intéressé pourrait compromettre l'exactitude du renseignement ou l'accès à celui-ci, et que les fins soulevées par l'employeur sont suffisamment légitimes et importantes; ou (iii) si l'employeur est victime d'un problème sérieux en lien avec l'utilisation d'Internet au travail, et que les fins soulevées par l'employeur sont suffisamment légitimes et importantes pour justifier que la surveillance soit effectuée au su et avec le consentement des employés.

---

[525] *Supra*, p. 78 et suiv.

Voyons maintenant en quoi consistent ces trois exceptions.

3.2.1.3.2. L'EXISTENCE D'UNE FAIBLE EXPECTATIVE DE VIE PRIVÉE

Lorsque l'expectative de vie privée de l'employé à l'égard de l'utilisation d'Internet au travail est suffisamment faible, que la surveillance n'implique pas la collecte de renseignements personnels et que l'employeur a de bons motifs pour vouloir exercer une surveillance au niveau de cette utilisation, il est possible de considérer que l'employé a implicitement consenti à la surveillance. D'autres diront que dans les circonstances, l'employeur a un droit implicite de surveiller l'utilisation d'Internet de ses employés[526]. Le cas échéant, il n'est pas nécessaire d'informer les employés ni d'obtenir leur consentement pour que le critère de proportionnalité soit respecté.

En effet, il n'y a pas que la connaissance de la surveillance et sa reconnaissance par l'employé qui ont pour effet de réduire l'expectative de l'employé dans le cadre de l'utilisation d'Internet au travail. D'autres éléments liés au contexte de travail et à la nature de l'entreprise ou de l'emploi peuvent également entrer en ligne de compte et réduire l'expectative de vie privée de l'employé à un point tel que l'employeur sera justifié de surveiller l'utilisation d'Internet à l'insu et sans le consentement de l'employé[527].

Encore là, il n'y a pas ici de formule-clé pour déterminer les situations dans lesquelles l'expectative de vie privée est suffisamment faible pour que l'employeur puisse exercer la surveillance de l'utilisation d'Internet à l'insu et sans le consentement de l'employé, tout étant du cas d'espèce. Néanmoins, il est recommandé de s'inspirer des décisions jurisprudentielles rendues en matière de fouille des employés, lesquels

---

[526] Par analogie, il est possible de se référer aux principes établis en matière de fouille dans l'affaire *Syndicat international des travailleurs de la boulangerie, confiserie et du tabac, section locale 476 F.A.T.-C.I.O.-C.T.C. et Walter M. Lowney Co.*, préc., note 272, 675 (droit de fouille implicite en fonction de l'importance et de la nature des opérations de la compagnie); et L. BERNIER, L. GRANOSIK et J.-F. PEDNEAULT, préc., note 270, par.21.120 (nature de l'entreprise).

[527] *Supra*, p. 102 et suiv.

pourront généralement être appliquées *a fortiori*, compte tenu que l'expectative de vie privée de l'employé est en principe plus élevée à l'égard des fouilles qu'à l'égard de la surveillance de l'utilisation d'Internet.

3.2.1.3.3. L'ENQUÊTE MENÉE SUR LA BASE DE SOUPÇONS SUR UN EMPLOYÉ

Un employeur pourra également mettre en place une surveillance de son employé dans le cadre d'une enquête sur le comportement de ce dernier, et ce, à son insu et sans son consentement, si les conditions suivantes sont remplies : (i) la surveillance (incluant la collecte d'informations personnelles) effectuée au su et avec le consentement de l'intéressé pourrait compromettre l'exactitude du renseignement ou l'accès à celui-ci ; (ii) les fins invoquées par l'employeur sont suffisamment légitimes et importantes pour justifier que l'employeur soit soustrait à ces obligations ; et (ii) l'employeur est en mesure de démontrer qu'il a épuisé tous les autres recours à sa disposition pour obtenir les renseignements recherchés ou pour remédier au problème en utilisant des moyens moins envahissants, et limite le plus possible la surveillance à cette fin.

Cette exception est clairement prévue dans les lois sur la protection des renseignements personnels[528] et est notamment reconnue depuis longtemps par les tribunaux en matière de fouille des employés[529] et de filature des employés absents pour raison de santé[530].

---

[528] Loi sur le secteur privé, art. 6 al. 3; L.p.r.p., art. 5(3); L.p.r.p.d.é., art. 7(1)b) et 7(2)d) et annexe 1, principe 4.3. Pour des illustrations de l'exception en matière de surveillance vidéo dans l'application de la L.p.r.p.d.é., voir : COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumés de conclusions d'enquêtes en vertu de la LPRPDÉ n° 2004-268, préc., note 457; n° 2004-269, préc., note 425; et n° 2007-379, préc., note 425.

[529] *Canapar Ltée et Fraternité nationale des charpentiers-menuisiers, forestiers, travailleurs d'usines*, préc., note 404; *Re Amalgamated Electric Corp. Ltd. (Markham) and International Brotherhood of Electrical Workers*, préc., note 471; *Re Inco Metals Co. and United Steelworkers* (1978), 18 L.A.C. (2d) 420 (Ont. Arbitration Board); *Re University Hospital and London & District Service Worker's Union*, préc., note 471; et Donald J. M. BROWN et David M. BEATTY, *Canadian Labour Arbitration*, 4th edition, Aurora (Ont.), Canada Law Books, 2006, feuilles mobiles, à jour au 23 mars 2009 (no.10, MAR:2009), no. 7:3625, p. 7-164 et 7-165.

[530] COMMISSION DES DROITS DE LA PERSONNE ET DE LA JEUNESSE, *Filature et surveillance des salariés absents pour raison de santé : conformité à la charte*, préc., note 409, p. 16. Pour des illustrations

Ainsi, si l'employeur ou son représentant surveillent et enregistrent sur le fait même un employé en train de mener des activités illégales sur Internet ou de contrevenir à ses obligations découlant de son contrat de travail, le fait de lui demander son consentement et de l'informer de la surveillance pour recueillir des renseignements le concernant pourrait alors compromettre la disponibilité et l'exactitude de l'information aux fins de l'enquête. Le cas échéant, les exemptions prévues pourraient s'appliquer.

Par ailleurs, les fins soulevées par l'employeur doivent être suffisamment légitimes et les soupçons de l'employeur suffisamment sérieux pour justifier la surveillance. Il ne sera pas suffisant que les faits allégués soient uniquement susceptibles de créer des doutes ou concernent uniquement un problème potentiel. Il faudra plutôt que les soupçons de l'employeur soient fondés sur des doutes suffisamment sérieux[531].

Par ailleurs, si l'employeur reçoit une plainte de discrimination ou de harcèlement au sujet d'un de ses employés, il a l'obligation de traiter cette plainte et de prendre les mesures réparatrices efficaces pour éliminer les conditions peu souhaitables pouvant exister au sein de l'entreprise[532]. Dans ce contexte, et sous réserve que la surveillance soit une solution efficace et nécessaire pour résoudre le problème, l'employeur pourrait invoquer la présente exception pour effectuer une surveillance ciblée des activités Internet de l'employé concerné.

Si une plainte ou des doutes sérieux concernent un acte interdit ou illégal considéré suffisamment sérieux et important pour justifier une surveillance des activités Internet d'un ou de plusieurs employés, l'employeur pourra invoquer la présente exception et

---

jurisprudentielles de ce principe, voir : *Godbout* c. *Ville de Longueuil*, préc., note 174; *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 117; *Syndicat des employés municipaux de la Ville de Saguenay (CSN) et Saguenay (Ville de)*, préc., note 243; *Genest et Québec (Directeur général des élections)*, préc., note 402; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2004-269, préc., note 425.

[531] *Supra*, p. 137.

[532] *Robichaud* c. *Canada (Conseil du trésor)*, préc., note 62.

se livrer à une telle surveillance à l'insu et sans le consentement de l'employé, sous réserve que l'atteinte soit minimale et qu'aucun autre moyen moins intrusif ne puisse permettre à l'employeur de remplir ses obligations[533].

Bien que dans l'affaire *Syndicat canadien des communications, de l'énergie et du papier, section locale 522 et C.A.E. Électronique ltée*[534] l'employé n'ait pas contesté la surveillance exercée par l'employeur, les faits de cette affaire offrent un bon exemple de situation dans laquelle la présente exception pourrait être soulevée. En l'espèce, l'employeur a mené une enquête quant aux activités Internet d'un employé sur lequel il entretenait de sérieux soupçons de vols de temps et d'activités contraires aux politiques de la compagnie (pornographie). L'employeur avait graduellement observé que l'employé encourait du retard dans son travail alors qu'il effectuait pourtant beaucoup d'heures de travail en temps supplémentaire. Il avait également constaté que l'employé passait beaucoup de temps à son ordinateur et que le plaignant faisait usage de l'internet sur son ordinateur, alors que cet usage n'était pas requis pour son travail. Ces éléments ayant fondé ses soupçons, il a fait sortir les rapports des activités Internet de l'employé, lesquels ont révélé que l'employé avait passé plus de 293 heures à naviguer sur Internet pendant ses heures de travail et qu'une grande proportion des sites visités représentaient des sites pornographiques. Selon le tribunal, l'employeur avait eu raison de surveiller les activités Internet de son employé, tel qu'il ressort des propos de l'arbitre Me Jean-Pierre Tremblay :

> « Quant à l'usage personnel que faisait le plaignant de l'internet, on pourrait le comparer d'une certaine façon avec l'usage d'un téléphone ; s'il est démontré que l'usage qui en est fait par l'employé ne l'est pas à des fins d'exécution du travail, il y a un problème qui peut justifier une intervention plus soutenue de l'employeur à des fins d'enquête ; si l'employeur doit en effet avoir des motifs sérieux pour mettre sous surveillance un employé, c'est généralement le résultat de l'enquête qui démontrera s'il y avait uns justification objective à celle-ci. »[535]

---

[533] Par analogie avec les principes énoncés dans COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Des plaintes de harcèlement et de vandalisme justifient une surveillance* (2006-2007), en ligne : http://www.priv.gc.ca/cf-dc/pa/2006-07/pa_200607_05_f.cfm.

[534] Préc., note 95.

[535] *Id.*, 334.

3.2.1.3.4. LA SURVENANCE D'UN PROBLÈME SÉRIEUX AU SEIN DE L'ENTREPRISE

Par analogie avec les principes établis en matière de fouilles et de protection des renseignements personnels, il apparaît que l'employeur peut également exercer une surveillance de l'utilisation d'Internet à l'insu et sans le consentement de l'employé si les conditions suivantes sont remplies : (i) l'employeur a subi de nombreux dommages liés à une mauvaise utilisation d'Internet par les employés de son entreprise; (ii) le problème de l'employeur est suffisamment légitime et important; et (iii) l'employeur est en mesure de démontrer qu'il a épuisé tous les autres recours à sa disposition pour obtenir les renseignements recherchés ou pour remédier au problème en utilisant des moyens moins envahissants, et limite le plus possible la surveillance à cette fin.

La présente exception se distingue de la précédente en ce que la surveillance n'a pas lieu dans le cadre d'une enquête sur un ou plusieurs employés, mais vise plutôt à enrayer un problème général.

Le test appliqué pour reconnaître un problème comme suffisamment légitime et important pour justifier une surveillance de l'utilisation d'Internet à l'insu et sans le consentement de l'employé est assez sévère[536] et est sensiblement le même que celui applicable dans le cadre de l'exception précédente. Ce sont d'ailleurs les mêmes dispositions législatives en matière de protection des renseignements personnels qui s'appliquent dans les deux cas[537].

---

[536] Par analogie avec les principes énoncés en matière de fouille par B. TURMEL, préc., note 404, à la page 61. Pour des illustrations jurisprudentielles de la sévérité du test dans le cadre d'épidémies de vols au travail, voir : *Syndicat international des travailleurs de la boulangerie, confiserie et du tabac, section locale 476 F.A.T.-C.I.O.-C.T.C. et Walter M. Lowney Co.*, préc., note 272, 675 ; *Canapar Ltée et Fraternité nationale des charpentiers-menuisiers, forestiers, travailleurs d'usines*, préc., note 404, 610; et *Re United Automobile Workers, local 444 and Chrysler Corporation of Canada Limited*, préc., note 488, 160.

[537] Loi sur l'accès, art. 65 al. 5; Loi sur le secteur privé, art. 6 al. 3; L.p.r.p., art. 5(3); et L.p.r.p.d.é., art. 7(1)b) et 7(2)d) et annexe 1, principe 4.3.

Pour illustrer la présente exception, nous pouvons appliquer par analogie les principes énoncés dans l'affaire *Bombardier-Canadair et Association internationale des machinistes et des travailleurs de l'aérospatiale, loge d'avionnerie de Montréal, section locale 712*[538], dans laquelle un employé avait délibérément bloqué, et ce à plusieurs reprises, la toilette de l'employeur. La preuve des incidents intérieurs avait été clairement établie devant la Cour et il était clair que l'employeur avait intérêt à faire cesser les dommages à sa propriété. De plus, la mise en place d'une caméra cachée était le seul moyen de découvrir la personne déloyale et de garder la salle de bain propre. En l'espèce, l'arbitre a jugé que l'objectif de l'employeur était suffisamment important pour justifier la mise en place d'une telle surveillance, et ce malgré le fait qu'elle se faisait dans un endroit où les employés disposent d'une importante expectative de vie privée, et malgré le fait que cette surveillance s'est faite à leur insu et sans leur consentement.

Dans une situation similaire, la CPVPC a conclu que l'entreprise n'avait pas satisfait aux exigences de l'article 5(3) L.p.r.p.d.é. pour invoquer les alinéas 7(1)b) et 7(2)b) de la L.p.r.p.d.é., pour le motif que l'entreprise n'avait pas épuisé toutes les mesures à sa disposition pour enrayer le problème et qui portaient moins atteinte à la vie privée des employés[539]. Il est donc important que toutes les conditions soient respectées pour que l'exception puisse s'appliquer.

Une autre illustration de l'application de cette exception se retrouve dans l'arrêt *Eastmond c. Canadian Pacific Railway*[540], également en matière de protection des renseignements personnels. En l'espèce, la Cour fédérale devait déterminer si la surveillance vidéo respectait l'article 5(3) de la L.p.r.p.d.é.. Pour établir que la surveillance était justifiée par des intérêts importants et donc raisonnables, l'employeur alléguait plusieurs incidents de vandalisme lui ayant causé plusieurs

---

[538] Préc., note 401.

[539] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2007-379, préc., note 425.

[540] Préc., note 363.

centaines de milliers de dollars de dommages. La Cour a conclu comme suit :

> « D'après la preuve, je suis convaincu que CP a établi la nécessité légitime de faire installer les caméras aux endroits où elles se trouvaient et d'enregistrer l'image des personnes traversant leur champ de vision fixe. (...) je suis persuadé, selon l'ensemble de la preuve, que CP a décelé dans le passé de nombreux incidents qui justifient la nécessité de poser des caméras de surveillance. »[541]

En matière d'utilisation d'Internet au travail, l'employeur pourra notamment invoquer cette exception s'il est victime de dissémination d'information confidentielle par voie de courrier électronique, si un important problème de harcèlement sexuel est relaté au sein de l'entreprise ou si toutes autres activités illégales ou préjudiciables sont menées par le biais de l'utilisation d'Internet au travail, sans toutefois que l'employeur puisse attribuer les incidents ou les plaintes à un employé ou à un groupe d'employés en particulier et sous réserve qu'il n'ait pas d'autres moyens moins intrusifs à sa disposition pour identifier le ou les employés fautifs ou régler le problème.

3.2.1.4. Les obligations d'information et de consentement à l'égard des tiers

Tel qu'exposé précédemment, l'employeur peut, par le biais de la surveillance de l'utilisation d'Internet, porter atteinte à la vie privée des tiers et collecter des renseignements personnels les concernant. Encore une fois, l'obligation d'information et de consentement de l'employeur va dépendre en grande partie de l'expectative de vie privée de ces tierces personnes lorsqu'elles entrent en communication avec des employés de l'organisme, et des renseignements personnels qui sont collectés sur ces tiers au cours de la surveillance.

Si ces tiers disposent en effet d'une expectative raisonnable de vie privée ou si

---

[541] *Id.*, par. 177. Voir également l'affaire *St. Mary's Hospital* and *H.E.U. (Re)* (1997), 64 L.A.C. (4th) 382 (Ont. Arbitration Board) en matière de surveillance vidéo. Il s'agissait en l'espèce d'un grief entrepris par le syndicat afin de contester la surveillance des employés de l'hôpital. La surveillance avait été mise en place dans le sous-sol de l'hôpital à la suite de problèmes de vol et de vandalisme. L'hôpital avait bien précisé qu'il ne s'agissait pas de surveiller la productivité des employés, mais plutôt d'une mesure de sécurité mise en place suite aux incidents survenus antérieurement. Selon l'arbitre, l'hôpital faisait face à un sérieux problème de vandalisme et de vol et était justifié d'exercer la surveillance.

l'employeur collecte des renseignements personnels les concernant, il apparaît que l'employeur devra faire un effort raisonnable pour les informer de la surveillance et de la collecte de renseignements personnels, et pour obtenir leur consentement.

Le Commissariat à la protection de la vie privée du Canada a d'ailleurs rappelé à plusieurs reprises le fait que l'enregistrement de communications des employés au travail pouvait impliquer la collecte de renseignements personnels concernant des tiers, notamment des clients, et que par conséquent, les entreprises étaient tenues d'informer les clients du fait que leurs communications pouvaient être enregistrées et des raisons qui motivaient cette mesure[542].

Pour aviser les tiers, l'employeur pourra par exemple inclure l'avis suivant à la fin de chacun des messages transmis par courrier électronique à partir de l'entreprise :

> « AVIS RELATIF AUX RENSEIGNEMENTS PERSONNELS
>
> Veuillez prendre note qu'afin de diminuer les risques liés à l'utilisation d'Internet au travail, plus particulièrement (...énoncer les fins...) la sécurité du réseau, la dissémination d'information privilégiée et la circulation de contenu préjudiciable et illégal sur le réseau, ce courriel et tout document qui y est annexé sont enregistrés. Par conséquent, tout renseignement personnel contenu dans ce courriel et tout document qui y est annexé pourrait être collecté, utilisé ou communiqué par l'entreprise. Veuillez prendre note que la collecte, l'utilisation et la communication de tout renseignement personnel par l'entreprise se fait uniquement aux fins déterminées et que tout document personnel sera détruit lorsque sa conservation ne sera plus nécessaire pour la réalisation des fins déterminées. Pour plus de renseignements, vous pouvez consulter notre politique de vie privée, disponible à l'adresse suivante : www.nomdedomaine.ca »

Mis à part les communications par courrier électronique, il ne sera pas toujours évident pour un employeur de remplir son obligation d'information et de consentement à l'égard des tiers dans le cadre de la surveillance de l'utilisation d'Internet, d'autant plus que l'atteinte au tiers ou la collecte de renseignements

---

[542] Voir notamment COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2007-387, préc., note 497; et COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Fiche d'information-Lignes directrices sur l'enregistrement des appels téléphoniques des clients,* révisé en juin 2008, en ligne : http://www.priv.gc.ca/fs-fi/02_05_d_14_f.cfm.

personnels le concernant sont généralement des éléments accessoires et inévitables lors de la surveillance de l'employé.

À cet égard, la L.p.r.p.d.é. contient une réserve pouvant être invoquée par les employeurs en matière de protection des renseignements personnels lorsqu'il leur est impossible ou inopportun d'informer les tiers de l'exercice de la surveillance. Le troisième principe de l'Annexe 1 de la L.p.r.p.d.é. énonce ce qui suit à l'égard des personnes avec lesquelles l'organisation n'entretient aucune relation directe :

> « **4.3 Troisième principe — Consentement**. Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.
>
> Note : Dans certaines circonstances, il est possible de recueillir, d'utiliser et de communiquer des renseignements à l'insu de la personne concernée et sans son consentement. (...) De plus, les organisations qui ne sont pas en relation directe avec la personne concernée ne sont pas toujours en mesure d'obtenir le consentement prévu. Par exemple, il peut être peu réaliste pour une œuvre de bienfaisance ou une entreprise de marketing direct souhaitant acquérir une liste d'envoi d'une autre organisation de chercher à obtenir le consentement des personnes concernées. » (nos soulignés)

Bien que cette réserve ne se retrouve pas expressément dans les lois sur la protection des renseignements personnels ni du secteur public ni de compétence québécoise, elle pourrait néanmoins être invoquée si l'employeur justifie un intérêt suffisamment légitime ou important[543]. Le même principe s'applique également en matière de vie privée, sous réserve que les critères de rationalité et de proportionnalité soient respectés.

De plus, à la lumière des principes établis en matière d'enregistrement des appels téléphoniques des clients, il semblerait que l'obligation d'information et de consentement à l'égard des tiers ne soit pas très sévère. En effet, dans des conclusions

---

[543] Loi sur le secteur privé, art. 6, al.3; L.p.r.p., art. 5(1) et art. 8(2)m). La Loi sur l'accès ne contient toutefois aucune disposition semblable.

d'enquête en vertu de la L.p.r.p.d.é.[544], le Commissaire a conclu, à l'égard d'une entreprise de télécommunication qui enregistrait les appels de ses téléphonistes à des fins d'assurance de la qualité, que celle-ci n'était pas tenue, en vertu de la loi, d'informer ses clients du fait que les appels étaient enregistrés et que l'entreprise ne contrevenait pas au principe 4.3 de l'annexe 1 de la L.p.r.p.d.é.

Ce raisonnement est d'ailleurs logique. Une entreprise qui surveille l'utilisation d'Internet au travail concentre généralement son attention sur l'employé et sur sa manière de travailler par le biais d'Internet. Elle ne s'attardera pas sur les renseignements concernant le tiers et ses objectifs ne seront pas en lien avec cette tierce personne. Le fait que des renseignements personnels sur un tiers soient collectés en même temps que l'enregistrement des communications de l'employé est un élément strictement accessoire et les renseignements personnels fournis par le tiers ne seront en principe utilisés que pour donner le service demandé (s'il s'agit d'un client ou un partenaire), ou encore à des fins personnelles par l'employé (s'il s'agit d'un proche).

Par conséquent, à l'égard des tiers, il est recommandé à l'employeur de s'en tenir à l'avis dans les messages électroniques, tel que mentionné précédemment.

3.3. L'adoption d'une politique de surveillance et d'utilisation d'Internet

3.3.1. Généralités

En matière de surveillance de l'utilisation d'Internet au travail, l'employeur n'a pas l'obligation d'adopter une politique de surveillance ou une politique d'utilisation d'Internet au travail. Un tribunal ne pourra conclure qu'un employeur a exercé illégalement une surveillance de l'utilisation d'Internet du seul fait qu'il n'a pas préalablement adopté de telles politiques.

---

[544] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2003-160 – *Une entreprise de télécommunications surveillance les appels des clients*, en ligne : http://www.priv.gc.ca/cf-dc/2003/cf-dc_030416_5_f.cfm.

Néanmoins, il est fortement recommandé aux employeurs de regrouper les informations sur la surveillance et sur l'usage permis d'Internet dans une directive ou une politique sous un format facile à consulter, que chaque employé reçoive copie de cette politique et y consente expressément. La doctrine recommande d'ailleurs fortement à toute organisation qui collecte des renseignements personnels de se doter de politiques claires à cet égard :

> « Peu importe le mode de cueillette ou d'interception d'information, il est essentiel que les entreprises se dotent de politiques claires à cet égard. Les employés doivent connaître les moyens utilisés par l'employeur pour recueillir l'information les concernant et l'usage qui sera fait de ces renseignements. »[545]

Notre intention n'est pas ici d'exposer en détails les principes entourant les politiques de surveillance ou d'utilisation d'Internet, ce sujet pouvant à lui seul faire l'objet d'un travail de recherche. Nous tenons simplement à sensibiliser les employeurs quant à l'importance et aux avantages de telles politiques lorsqu'il est question de surveillance de l'utilisation d'Internet.

3.3.2. Avantages d'une politique

L'adoption d'une politique de surveillance de l'utilisation d'Internet et son approbation par les employés ou le syndicat permettra non seulement à l'employeur de satisfaire ses obligations d'information et de consentement, mais également de réduire l'expectative raisonnable de vie privée de l'employé[546], sans oublier qu'elle constituera un outil de gestion et de référence essentiel tant pour l'employeur que pour les employés. Il est donc grandement utile pour un employeur de se doter d'une telle politique.

---

[545] Lyne DUHAIME, « La protection des renseignements personnels en milieu de travail », dans S.F.P.B.Q., vol. 258, *Vie privée et protection des renseignements personnels (2006)*, Cowansville, Éditions Yvon Blais, p. 83, à la page 65. Voir également : K. DELWAIDE, « L'Internet en milieu de travail et les politiques et directives relatives à l'utilisation des nouvelles technologies », préc., note 53, p. 32; C.H.H. MCNAIRN et A. K. SCOTT, *Privacy Law in Canada*, préc., note 255, p. 179; D. VEILLEUX, préc., note 241, à la page 43; COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 2004-269, préc., note 425; et COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Fiche d'information - La protection des renseignements personnels au travail*, préc., note 483.

[546] *Supra*, p. 83 et suiv.

En matière de surveillance de l'utilisation d'Internet au travail, ce principe est notamment illustré dans l'affaire *Blais et La Société des Loteries Vidéos du Québec Inc.*[547] précitée. En effet, dans cette affaire, l'existence d'une politique sur le courrier électronique précisant les mesures de suivi et de contrôle assurées par le gestionnaire du réseau de la compagnie quant à l'utilisation de cet outil au travail, a été l'un des facteurs déterminant dans la conclusion de la Commission à l'effet que l'employé ne disposait, dans les circonstances, d'aucune expectative raisonnable de vie privée à l'égard de ses échanges électroniques.

Par ailleurs, en matière de fouille des courriers électroniques au travail, dans l'affaire *Briar* c. *Conseil du Trésor (Solliciteur général du Canada - Service correctionnel)*[548], la Commission des relations de travail dans la fonction publique du Canada a mis beaucoup d'importance sur le fait que plusieurs politiques, mémos et avertissements à l'effet que le système informatique était surveillé par l'employeur avaient circulés auprès des employés, pour conclure que la fouille de l'employeur dans la boîte de courrier électronique n'avait pas enfreint la vie privée des employés :

> « Compte tenu de la politique de l'employeur interdisant l'utilisation du système de courrier électronique à des fins inacceptables et de l'existence d'un avertissement clair, à l'entrée en communication, que le système est surveillé conformément à cette politique, il est difficile de comprendre comment les fonctionnaires s'estimant lésés peuvent prétendre qu'on a porté atteinte à leur vie privée dans ces circonstances »[549]

Par ailleurs, une politique de surveillance de l'utilisation d'Internet renforce d'autant plus le droit de surveillance de l'employeur si elle est négociée et approuvée par le syndicat de l'organisation, ou encore si elle est utilisée durant un certain nombre d'années sans avoir fait l'objet de contestation par un ou des employés de

---

[547] Préc., note 136.

[548] Préc., note 327.

[549] *Id.*, par. 59.

l'organisation[550].

3.3.3. Contenu d'une politique

Quant au contenu de la politique, les éléments essentiels devant y être mentionnés sont ceux mentionnés à la section 3.2.1.2.1.[551] quant à l'étendue de l'obligation d'information. En outre, il est recommandé à l'employeur d'inclure les éléments suivants : (i) les lignes directrices au niveau de la gestion des renseignements personnels ou confidentiels collectés par le biais de la surveillance, y compris leur sécurité, leur utilisation, leur communication et leur conservation; (ii) la marche à suivre pour toute personne qui souhaite consulter ses renseignements personnels collectés au cours de la surveillance ou contester l'exactitude et la complétude des renseignements personnels détenus par l'organisation; (iii) la marche à suivre pour toute personne qui souhaite déposer une plainte auprès de l'entreprise concernant la manière dont la surveillance est exercée ou que les renseignements personnels sont collectés, utilisés, communiqués ou conservés ; (iv) le nom des personnes autorisées à exploiter le système de surveillance et à consulter les renseignements qu'il contient; (v) le nom ou la fonction de même que l'adresse de la personne responsable de la politique de surveillance et des pratiques de protection des renseignements personnels collectés dans le cadre de la surveillance ; et (vi) le nom ou la fonction de même que l'adresse de la personne à qui les demandes de communication des renseignements personnels doivent être acheminées.

Par ailleurs, il est important que les personnes qui rédigent les politiques comprennent que le contenu de la politique doit être adapté en fonction de nombreux facteurs, dont la nature de l'organisation et de l'emploi, le contexte de travail, les fins poursuivies par l'employeur et les types de renseignements collectés dans le cadre de la surveillance.

---

[550] *Re United Automobile Workers, local 444 and Chrysler Corporation of Canada Limited*, préc., note 488; et C.H.H. MCNAIRN et A. K. SCOTT, *Privacy Law in Canada*, préc., note 255, p. 180.

[551] *Supra*, p. 158.

Il est également recommandé que la politique de l'employeur prévoie les usages permis au niveau des services Internet mis à la disposition des employés, ou encore que l'employeur adopte, parallèlement à la politique de surveillance, une politique d'utilisation des services Internet, de manière à ce que les employés connaissent leurs devoirs et leurs limites dans le cadre l'utilisation du réseau Internet au travail. L'employeur pourra par exemple interdire expressément à ses employés le fait d'utiliser Internet à des fins personnelles, ou encore limiter l'usage personnel d'Internet aux périodes de pause.

L'adoption d'une politique d'utilisation d'Internet au travail et sa mise à la connaissance au niveau des employés permettra notamment à l'employeur de justifier plus facilement les sanctions disciplinaires prises contre les employés qui utilisent Internet à des fins non autorisées[552]. Au niveau du contenu d'une telle politique, les éléments essentiels devant y être mentionnés sont les suivants[553] : (i) un rappel à l'effet que l'accès Internet est mis à la disposition des employés aux fins de leur travail et non à des fins personnelles : (ii) les paramètres d'utilisation de l'accès Internet au travail et (iii) les conséquences d'un manquement aux termes de la politique (sanctions disciplinaires). Il est par ailleurs recommandé aux employeurs de rappeler aux employés que l'utilisation de l'accès Internet au travail doit se faire dans le respect de la dignité des autres et de manière à maintenir un environnement de travail exempt de discrimination et de harcèlement.

---

[552] L'existence d'une politique d'utilisation et sa connaissance effective au niveau des employés est l'un des facteurs considérés par les tribunaux québécois lorsqu'il s'agit de déterminer si l'employé a commis une faute grave dans le cadre de l'utilisation d'Internet au travail. Voir notamment : ; *Syndicat canadien des communications, de l'énergie et du papier, section locale 522 et C.A.E. Électronique ltée,* préc., note 95; *Commission des normes du travail* c. *Bourse de Montréal inc.*, préc., note 136; *Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada*, préc., note 136; *Syndicat canadien de la fonction publique, section locale 4140 et Centres jeunesse de l'Outaouais*, préc., note 97; *Syndicat des spécialistes et professionnels d'Hydro-Québec, section locale 4250 (SCFP-FTQ) et Hydro-Québec*, préc., note 96; *Syndicat de la fonction publique du Québec – Fonctionnaires et Québec (Ministère de l'Emploi et de la Solidarité sociale)*, préc., note 97. À l'égard des politiques d'utilisation d'Internet au travail, voir R. PERREAULT, préc., note 111, aux pages 74 et 96.

[553] R. PERREAULT, préc., note 111, aux pages 96 et 97; K. DELWAIDE, « L'Internet en milieu de travail et les politiques et directives relatives à l'utilisation des nouvelles technologies », préc., note 53, p. 48-51.

3.3.4. Autres conseils

Les politiques doivent être raisonnables, non discriminatoires, uniformes et claires. L'employeur doit s'assurer que la politique respecte les dispositions contenues dans les contrats de travail et la convention collective (s'il y a lieu), à défaut de quoi elle risque de faire l'objet d'un grief par le syndicat ou d'être déclarée invalide[554].

Ce principe est notamment illustré dans l'affaire *Association des professionnels de la Régie régionale de la santé et des services sociaux 002 (C.S.N.) et Régie régionale de la santé et des services sociaux du Saguenay—Lac-St-Jean*[555] à l'égard d'une politique d'utilisation d'Internet. En l'espèce, l'arbitre a confirmé qu'en adoptant unilatéralement cette politique, l'employeur avait modifié les conditions de travail de ses employés, et qu'en vertu de la convention collective, il aurait dû obtenir l'approbation préalable du syndicat. La politique a donc dû être modifiée[556].

Évidemment, l'adoption d'une politique de surveillance et sa mise à la connaissance au niveau des employés n'est pas le seul moyen pouvant être utilisé par l'employeur pour renforcer son droit de surveillance. L'employeur aura intérêt à s'assurer que les employés comprennent bien le contenu de la politique et à effectuer des rappels régulièrement quant à la pratique de la surveillance.

L'employeur pourra par exemple distribuer des dépliants aux employés résumant les termes et conditions contenus dans la politique ou la directive, ou encore organiser des séances d'information à l'intention des employés, de manière à s'assurer que ceux-ci comprennent bien tous les termes de la politique et puissent poser des questions quant à son contenu, si nécessaire.

---

[554] K. DELWAIDE, « L'Internet en milieu de travail et les politiques et directives relatives à l'utilisation des nouvelles technologies », préc., note 53, p. 47.

[555] [2002] R.J.D.T. 990, D.T.E. 2002T-444 (T.A.).

[556] *Id.*, 1002-1005. Voir également *Association des juristes de l'État et Commission des valeurs mobilières du Québec*, préc., note 391, par. 64. « Ainsi, considérant que la notion de condition de travail peut englober « toutes les questions qui touchent aux relations de travail », du moment qu'elles ne sont pas contraires à l'ordre public et à la loi, et que de telles conditions peuvent être unilatéralement édictées par l'employeur dans le cadre de politiques ou règlements, il y a lieu de reconnaître à ce titre le contenu de la Politique Internet. »

L'employeur pourra également établir un système de rappel de la politique ou d'avertissement dès l'utilisation des services Internet par les employés. Une des solutions retenues par plusieurs entreprises est d'insérer des messages d'avertissements qui apparaissent à l'écran de l'ordinateur de l'employé dès qu'il se branche aux services Internet, réitérant certaines grandes lignes de la politique et exigeant que l'employé acquiesce au contenu du message avant d'avoir accès à Internet[557]. D'autres entreprises feront circuler des mémos aux employés pour leur rappeler le contenu de la politique.

À la lumière des principes que nous venons d'énoncer, l'employeur qui entend adopter et mettre en œuvre une politique de surveillance de l'utilisation d'Internet au travail devra porter une attention particulière aux éléments suivants :

- adoption : respecter la convention collective et les contrats de travail ; négocier la politique ou à tout le moins donner la possibilité aux employés (ou aux cadres) de donner leur avis ou commentaires avant son adoption;

- contenu : adapter le contenu de la politique au contexte de l'entreprise et des fins recherchées ; respecter l'obligation d'information prévue dans les lois sur la protection des renseignements personnels ; inclure des règles quant à l'utilisation d'Internet au travail;

- connaissance : mettre la politique à la connaissance des employés de l'entreprise ; afficher des avis, distribuer des pamphlets, tenir des séances d'information auprès des employés afin que ceux-ci soient au courant des

---

[557] À titre d'exemple, dans *Briar* c. *Conseil du Trésor (Solliciteur général du Canada - Service correctionnel)*, préc., note 327, le message d'avertissement indiquait ce qui suit (par. 11) : « WARNING – AVERTISSEMENT : [Traduction] L'utilisation de ce système est réservée aux personnes autorisées seulement, et elle est surveillée conformément à la Politique du Conseil du Trésor et du Service correctionnel du Canada sur l'utilisation des réseaux électroniques. Les comportements inappropriés ou illégaux seront signalés et des mesures disciplinaires peuvent s'ensuivre. » Voir également : Karen L. CASSER, « Employers, Employees, E-mail and The Internet », *The Internet and Business : A Lawyer's Guide to the Emerging Legal Issues*, Washington D.C., The Computer Law Association Inc., 1996, p. 5.

raisons qui sous-tendent la politique de surveillance, et de la manière dont la surveillance est exercée ; obtenir un consentement écrit des employés à l'égard de la politique;

- application : appliquer la politique de manière raisonnable, non discriminatoire, continue et uniforme, et uniquement pour les fins pour lesquelles elle est instaurée ; former les gestionnaires qui ont recours à cette surveillance afin de s'assurer qu'ils utilisent la surveillance de façon appropriée.

CONCLUSION

À la lumière de ce qui précède, la mise en place d'une surveillance de l'utilisation d'Internet au travail exige plusieurs réflexions de la part de l'employeur, exige la recherche d'un équilibre entre les droits des employés, des tiers et les droits de l'employeur, et ne se résume pas simplement à l'adoption d'une politique de surveillance ou encore à la propriété des outils informatiques de l'employeur.

L'employeur dispose bien d'un droit de surveillance, lequel est fondé sur son pouvoir de direction en vertu duquel il peut contrôler le travail de ses employés pendant leur temps de travail. Toutefois, ce droit ne peut être exercé de n'importe quelle façon. L'espace réservé aux droits des employés au Québec est en effet beaucoup plus important qu'on ne semble le croire et l'employeur qui décide de mettre en place une surveillance de l'utilisation d'Internet au travail doit s'assurer de respecter tant le droit à la vie privée des employés que leur droit à des conditions de travail justes et raisonnables.

Pour atteindre et maintenir un équilibre entre les différents intérêts en jeu, l'employeur qui met en place une surveillance de l'utilisation d'Internet au travail doit franchir deux étapes de réflexions. Il doit en premier lieu déterminer le niveau d'expectative raisonnable de vie privée du ou des employés surveillés dans l'utilisation d'Internet au travail, et ensuite analyser les critères du droit de surveillance à la lumière des circonstances.

Jusqu'à aujourd'hui, aucun tribunal québécois n'a conclu à l'existence d'une expectative raisonnable de vie privée d'un employé dans l'utilisation d'Internet au travail. Ceci ne doit toutefois pas laisser croire à l'employeur que ses employés ne disposent en aucun cas d'un droit à la vie privée dans le cadre des activités Internet qu'ils mènent au travail. En effet, la plupart des employés qui disposent de l'accès Internet dans le cadre de leur travail utilisent cet outil non seulement à des fins professionnelles, mais également à des fins personnelles. Dans ce contexte, et sous réserve des facteurs applicables, les employés peuvent raisonnablement s'attendre à

ce que leurs communications personnelles ou l'historique des sites web qu'ils ont visités ou des fichiers qu'ils ont téléchargés demeurent secrets ou privés.

Nous avons vu, dans le cadre du deuxième chapitre, que les facteurs applicables pour déterminer le niveau d'expectative raisonnable de vie privée d'un employé dans l'utilisation d'Internet au travail incluent notamment la connaissance de la surveillance, le consentement donné par l'employé à l'égard de la surveillance, la nature vulnérable des communications Internet, l'environnement de travail et la nature personnelle des communications surveillées.

Bien que plusieurs de ces facteurs soient indépendants de la volonté de l'employeur, ce dernier peut faire diminuer le niveau d'expectative de vie privée de ses employés en prenant certaines des mesures de transparence en parallèle à la mise en place de la surveillance de l'utilisation d'Internet. L'employeur peut par exemple adopter une politique de surveillance de l'utilisation d'Internet et la porter à la connaissance de ses employés, ou encore obtenir leur consentement écrit à l'égard de la surveillance. L'adoption de ces mesures renforcera en quelque sorte son droit de surveillance.

Une fois que l'employeur a déterminé si le ou les employés surveillés disposent ou non d'une expectative raisonnable de vie privée dans l'utilisation d'Internet au travail, l'employeur doit passer à la deuxième étape de réflexion, à savoir s'il respecte les critères du droit de surveillance, plus particulièrement les critères de rationalité et de proportionnalité.

L'analyse du critère de rationalité dans le contexte d'une surveillance de l'utilisation d'Internet au travail exige que l'employeur ne viole pas inutilement les droits des personnes surveillées et que les fins soulevées par l'employeur soient suffisamment légitimes et importantes pour justifier l'employeur de porter atteinte à ces droits. À cet égard, nous avons vu, dans le cadre du premier chapitre, que l'employeur peut avoir un ou plusieurs motifs de vouloir surveiller l'utilisation d'Internet de ses employés. Chacun de ces motifs a un niveau de légitimité variable, dépendamment de son rapprochement avec les intérêts économiques de l'entreprise. Quant à

l'importance des motifs soulevés par l'employeur, celle-ci variera en fonction des incidents subis par l'employeur et des doutes que ce dernier entretient à l'égard de l'employé ou des employés surveillés. Si l'employeur a subi des incidents sérieux et dommageables, ou encore s'il entretient des doutes sérieux sur un ou des employés par rapport à un problème important, l'objectif pourra être considéré comme suffisamment important. Ce qu'il faut retenir c'est que l'employeur ne peut mettre en place une surveillance de l'utilisation d'Internet sur la base d'un simple problème potentiel, sur la base de doutes non fondés, ou encore s'il ne souffre pas de réels dommages.

Le niveau de légitimité et d'importance requis pour que les fins soulevées par l'employeur respectent le critère de rationalité dépend en grande partie des éléments suivants : (i) du niveau d'expectative de vie privée de l'employé ou des employés surveillés; et (ii) de la manière dont l'employeur entend exercer la surveillance de l'utilisation d'Internet au travail. Plus le niveau d'expectative de l'employé est élevé, ou encore plus la manière dont l'employeur mène la surveillance est intrusive ou se compare à une forme de harcèlement, plus les fins soulevées par l'employeur doivent être légitimes et importants.

Quant au critère de proportionnalité, il exige que l'atteinte aux droits des employés ou des tiers soit minimale. À cet égard, la surveillance doit en premier lieu être nécessaire et permettre d'atteindre le ou les objectifs recherchés par l'employeur qui doit notamment avoir épuisé tous les autres recours moins intrusifs pour régler son problème.

Par ailleurs, le critère de proportionnalité est fortement lié à la manière dont l'employeur entend exercer la surveillance de l'utilisation d'Internet au travail et aux mesures de transparence prises en parallèle par l'employeur. Plus la surveillance s'étend à l'ensemble des employés et des activités Internet, ou encore plus elle est exercée de manière constante et permanente, plus l'employeur risque de porter atteinte aux droits des personnes surveillées. L'employeur a donc intérêt à se poser les questions requises quant à la manière dont la surveillance sera menée.

Une fois ces deux étapes franchies, l'employeur sera en mesure de déterminer si la surveillance respecte les droits des personnes surveillées et s'il doit, préalablement à la mise en place de la surveillance, remplir certaines obligations. Dépendamment des circonstances, l'employeur pourrait notamment avoir à informer le ou les employés surveillés et à obtenir leur consentement à l'égard de la surveillance.

L'adoption d'une politique de surveillance de même que l'obtention d'un consentement de la part du ou des employés à l'égard de la surveillance ne sont pas des mesures qui, une fois prises, donnent le droit à l'employeur de surveiller l'utilisation d'Internet de ses employés. L'adoption d'une politique et l'obtention du consentement constituent plutôt des mesures permettant à l'employeur de réduire le niveau d'expectative raisonnable de vie privée du ou des employés surveillés et de renforcer son droit de surveillance dans le cadre de l'analyse du critère de proportionnalité.

Notons par ailleurs que dans certaines situations, notamment lorsque le ou les employés surveillés disposent d'une expectative raisonnable de vie privée dans le cadre de leurs activités Internet, ou encore lorsque, par le biais de la surveillance, l'employeur collecte des renseignements personnels sur ses employés, l'employeur aura l'obligation d'informer les employés et d'obtenir leur consentement à l'égard de la surveillance. Dans ce contexte, l'adoption d'une politique et la signature d'un formulaire de consentement sont probablement les meilleurs moyens pour remplir ces obligations.

Les obligations d'information et de consentement peuvent par ailleurs être sujettes à certaines exceptions, notamment lorsque l'employé dispose d'une faible expectative raisonnable de vie privée, lorsque le respect de ces obligations risque de compromettre l'exactitude des renseignements qu'on vise à obtenir, ou encore lorsque l'employeur est victime d'un problème sérieux en lien avec l'utilisation d'Internet au travail. Dans les deux derniers cas, l'exception sera conditionnelle à ce que les fins soulevées par l'employeur soient suffisamment légitimes et importantes pour justifier la surveillance au su et sans le consentement du ou des employés surveillés.

Quant aux tiers qui entrent en communication avec les employés par le biais d'Internet, ceux-ci peuvent également, au même titre que les employés, disposer d'une expectative raisonnable de vie privée dans le cadre de leurs communications avec l'employé, ou encore voir leurs renseignements personnels collectés par l'employeur dans le cadre de la surveillance au travail. La personne qui écrit à son conjoint à l'adresse de courriel professionnel de ce dernier pour lui raconter un problème familial survenu au cours de la journée pourra, à moins d'indications contraires, raisonnablement s'attendre à ce que le message ne soit pas lu par l'employeur de son conjoint. Il est donc recommandé aux employeurs de tenir compte des droits des tiers lors de la mise en place d'une surveillance de l'utilisation d'Internet et de prévenir ces derniers, sous la forme par exemple d'avis électroniques apparaissant dans les courriels, de l'existence de la surveillance.

Finalement, l'employeur ne doit pas négliger les obligations découlant des lois en matière de protection des renseignements personnels. Si, par le biais de la surveillance, l'employeur risque de collecter des renseignements personnels, il doit alors respecter toutes les obligations préalables à la collecte de renseignements personnels imposées par les lois applicables.

À la lumière de ces principes, nous constatons qu'il n'y a pas de recette clé en matière de surveillance de l'utilisation d'Internet. Les facteurs qui entrent en considération dans l'analyse de la légalité d'une surveillance sont trop nombreux pour établir des directives claires applicables à toutes les circonstances. Toutefois, les questions que l'employeur doit se poser lors de la mise en place d'une surveillance de l'utilisation d'Internet ainsi que les facteurs applicables sont les mêmes dans tous les cas. Si l'employeur omet de se poser ne serait-ce que l'une de ses questions, ou omet d'y répondre en se basant sur les principes et les facteurs que nous avons exposés, l'employeur risque alors de porter atteinte aux droits de ses employés. Pour s'assurer de ne négliger aucune étape, nous recommandons à l'employeur d'utiliser la liste de vérification annexée au présent mémoire.

À l'aide de cette liste, l'employeur pourra non seulement s'assurer de ne négliger

aucun facteur, mais possèdera toutes les indications nécessaires quant aux étapes à suivre et aux mesures à prendre pour renforcer son droit de surveillance. Il s'agit donc en quelque sorte d'un mini-guide qui synthétise les principes applicables à chacune des étapes de la mise en place de la surveillance.

À la lumière de ce tableau et des principes exposés, la surveillance de l'utilisation d'Internet au travail paraît rigidement encadrée. Pourtant, une analyse de la jurisprudence québécoise révèle que les employés n'invoquent que très rarement leur droit à la vie privée ou à la protection de leurs renseignements personnels lorsqu'ils font l'objet de mesures disciplinaires suite à l'exercice d'une surveillance électronique. À cet égard, nous pourrions croire que les employés sont mal informés de leurs droits et qu'une certaine sensibilisation au niveau des enjeux de la surveillance électronique serait de mise, tant au niveau des employeurs qui croient pouvoir exercer une surveillance électronique selon leur bon vouloir, qu'au niveau des employés qui pourraient ainsi mieux faire valoir leurs droits.

Ce qui est désolant, mais qui constitue malheureusement une réalité dans notre société actuelle, c'est que le droit n'évolue pas du tout à la même vitesse que les technologies de surveillance au travail, et ce au détriment des droits des personnes surveillées.

À l'égard de l'évolution rapide des technologies de surveillance, nous pouvons citer notamment les « poussières intelligentes » (*Smart Dust* en anglais), des micro-capteurs invisibles à l'œil nu utilisés pour surveiller les déplacements des gens ou des objets. Les poussières d'identification (*ID-Dust*) sont un exemple de l'implantation de cette technologie. L'idée des poussières d'identification est de les saupoudrer à même le sol afin qu'elles se collent aux semelles des personnes qui se trouvent sur les lieux et ce, à leur insu, permettant ensuite de suivre leurs déplacements. Un autre exemple de l'implantation de cette technologie est la puce RFID (*Radio Frequency Identification*). De la grandeur d'un grain de riz, elle peut être implantée dans le corps même des employés pour remplacer leur badge d'accès. Cette pratique soulève bien évidemment plusieurs débats éthiques et juridiques, et a notamment été bannie

dans plusieurs États américains. D'ailleurs, le risque que ces technologies comportent pour les droits des employés est énorme si l'on pense à tous les usages qu'un employeur pourrait être tenté d'en faire et ce, à l'insu des employés.

Ceci nous amène à nous poser la question à savoir jusqu'où l'employeur va-t-il aller pour surveiller ses employés. À cet égard, nous n'avons qu'à penser au brevet déposé par Microsoft en 2008 qui permet de mesurer en temps réel le rythme cardiaque, la respiration, la température du corps, l'expression faciale et la pression sanguine de l'utilisateur d'un ordinateur par l'intermédiaire de capteurs sans fil, technologie que plusieurs employeurs pourraient être tentés d'utiliser ne serait-ce que pour établir des statistiques liées à la performance, au taux de réussite ou à la fréquence des problèmes de l'utilisateur, ou encore pour déterminer quel employé est le plus apte à effectuer un travail en particulier.

Les technologies de surveillance des employés évoluent sans cesse, à un rythme tel que la communauté juridique n'a pas toujours le temps de les analyser à la lumière des différents intérêts en jeu. Ceci a pour résultat que des pratiques et croyances s'établissent en milieu de travail, que les employés sont mal informés et mal sensibilisés à l'égard de leurs droits, et qu'au bout du compte peu ou pas d'employés ou de syndicats contestent ces mesures ou remettent en doute leur légalité.

Tel qu'exposé au 3^{e} chapitre, une pratique de surveillance exercée de manière constante et uniforme pendant plusieurs années sans que les employés ou le syndicat ne l'aient contestée peut, au bout d'un certain nombre d'années, se transformer en une condition d'emploi pour les employés. Nous osons espérer que ce principe ne s'appliquera pas à l'égard des technologies de surveillance de l'utilisation d'Internet ni aux autres technologies de surveillance émergentes que nous venons de mentionner et ce, tant que les employés n'auront été réellement informés de leurs droits et que l'équilibre ne sera pas établi entre les différents intérêts en jeu. Dans ce contexte, nous espérons contribuer à faire évoluer le droit dans la bonne direction.

TABLES BIBLIOGRAPHIQUES

Table de la législation

Canada

Charte canadienne des droits et libertés, édictée comme l'annexe B de la *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.)

Code Criminel, L.R., 1985, ch. C-46

Décret d'exclusion visant des organisations de la province de Québec, DORS, 20043-374

Décret liant certains mandataires de Sa Majesté pour l'application de la partie 1 de la Loi sur la protection des renseignements personnels et les documents électroniques, DORS/2001-8

Loi canadienne des droits de la personne, L.R.C. 1985, c. H-6

Loi sur la protection des renseignements personnels, L.R., 1985, ch. P-21

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5

Loi sur le droit d'auteur, L.R.C. 1985 ch. C-42

Loi sur les brevets, L.R., 1985, ch. P-4

Québec

Charte des droits et libertés de la personne, L.R.Q., chapitre C-12

Code civil du Québec, L.Q. 1991, c. 64

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., c. A-2.1

Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., c. P-39.1

Loi sur le cadre juridique des technologies de l'information, L.R.Q., chapitre C-1.1

Loi sur les normes du travail, L.R.Q., chapitre N-1.1

* Les références électroniques mentionnées ci-après sont à jour au 29 juin 2009.

France

Loi no. 91-646 du 10 juillet 1991 relative au secret des correspondances par voie de télécommunication, JO n° 162 du 13 Juillet 1991, p. 9167 et 10 août 1991 (rectificatif), p. 10617

Textes internationaux

Convention de sauvegarde des droits de l'homme et des libertés fondamentales, 4 novembre 1950, S.T.E. n° 5 (entrée en vigueur le 3 septembre 1953)

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 28 janvier 1981, S.T.E. n° 108

Déclaration universelle des droits de l'homme, Rés. A.G. 217 (III), Doc. off. A.G. N.U., 3e sess., supp. n° 13, Doc. N.U. A/810 (1948)

Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontaliers de données à caractère personnel, 23 septembre 1980

Pacte international relatif aux droits civils et politiques, 16 décembre 1966, (1976) 999 R.T.N.U. 171

Table de la jurisprudence

Jurisprudence québécoise

Air Canada c. *Constant*, [2003] C.A.I. 710, J.E. 2003-1799 (C.S.). Inscription en appel, 2003-10-02 (C.A.), 500-09-013818-034

Allain c. *Caisse populaire Laval-des-Rapides,* [2005] C.A.I 25 (C.A.I.)

Alliance de la fonction publique du Canada et Musée des beaux-arts du Canada, [2003] R.J.D.T. 468, D.T.E. 2003T-89 (T.A.)

Ambaw et Bijoux Continental Inc., D.T.E. 98T-757 (C.T.)

Amziane c. *Bell Mobilité*, D.T.E. 2004T-849, J.E. 2004-1702 (C.S.)

Arpin c. *Grenier*, [2004] R.J.D.T. 613, J.E. 2004-1172, (C.Q.)

Association des juristes de l'État et Commission des valeurs mobilières du Québec, [2003] R.J.D.T. 579, D.T.E. 2003T-212 (T.A.)

Association des professionnels de la Régie régionale de la santé et des services sociaux 002 (C.S.N.) et Régie régionale de la santé et des services sociaux du Saguenay—Lac-St-Jean, [2002] R.J.D.T. 990, D.T.E. 2002T-444 (T.A.)

Association des techniciennes et techniciens en diététique du Québec et Centre hospitalier Côte-des-Neiges, [1993] T.A. 1021, D.T.E. 93T-1329

Association internationale des machinistes et des travailleuses et travailleurs de l'aérospatiale, section locale 2468 et Rolls-Royce Canada ltée, D.T.E. 2001T-153 (T.A.)

Aubry c. *Éditions Vice-Versa Inc.*, [1998] 1 R.C.S. 591

Banque de Montréal c. *Kuet Leong Ng*, [1989] 2 R.C.S. 429

Bélisle (Maison Dutrisac) c. *Association Les Naturalistes du Baptiste Lefebvre*, B.E. 2006BE-113 (C.Q.)

Bélisle et Municipalité de Rawdon, 2005 QCCRT 0453, D.T.E. 2005T-777

Bell Canada et Association canadienne des employés de téléphone, [2000] R.J.D.T. 358, D.T.E. 2000T-254 (T.A.)

Bellefeuille c. *Morisset*, [2007] R.J.Q. 796, J.E. 2007-899 (C.A.)

Bellerose c. *Université de Montréal*, [1986] C.A.I. 109, conf. par J.E. 89-350, [1988] C.A.I. 377 (C.Q.)

Blais et La Société des Loteries Vidéos du Québec Inc., [2003] R.J.D.T. 261, D.T.E. 2003T-178 (C.R.T.)

Bombardier inc. — Canadair et Association internationale des machinistes et des travailleurs de l'aérospatiale, loge d'avionnerie de Montréal, section locale 712, [1996] T.A. 251, D.T.E. 96T-375

Brown c. *Industrielle Alliance valeurs mobilières inc.*, 2007 QCCS 1602, AZ-50427179

Bureau d'études Archer inc. c. *Dessureault*, 2006 QCCA 1556, AZ-50399426

Cabiakman c. *Industrielle-Alliance Cie d'Assurance sur la Vie*, [2004] 3 R.C.S. 195

Canapar Ltée et Fraternité nationale des charpentiers-menuisiers, forestiers, travailleurs d'usines, [1985] T.A. 606, D.T.E. 85T-755

Centre hospitalier de Buckingham et Syndicat des technologues en radiologie du Québec (C.P.S.), D.T.E. 2002T-884 (T.A.)

Centre hospitalier régional de Trois-Rivières (Pavillon St-Joseph) et Syndicat professionnel des infirmières et infirmiers de Trois-Rivières (Syndicat des infirmières et infirmiers Mauricie—Coeur-du-Québec), [2006] R.J.D.T. 397, D.T.E. 2006T-209, (T.A.)

Collège Ahuntsic c. *Syndicat du personnel de soutien du Collège Ahuntsic*, D.T.E. 2007T-889 (T.A.)

Commission des droits de la personne c. *Habachi*, [1992] R.J.Q. 1439, D.T.E. 92T-634 (T.D.P.Q.), inf. en partie [1999] R.J.Q. 2522 (C.A.)

Commission des droits de la personne et des droits de la jeunesse c. *Entreprise conjointe Pichette*, Lambert, Somec, J.E. 2007-1607, D.T.E. 2007T-713 (T.D.P.Q.)

Commission des droits de la personne et des droits de la jeunesse c. *Centre maraîcher Eugène Guinois Jr inc.*, [2005] R.J.Q. 1315 (T.D.P.Q.)

Commission des normes du travail c. *Bourse de Montréal inc.*, [2002] R.J.Q. 807 (C.Q.)

Corp. Outils Québec et Syndicat indépendant des salariés de Outils Québec, [1992] T.A. 646, D.T.E. 92T-933

Curley c. *Latreille*, (C.S. Can., 1920-02-03), SOQUIJ AZ-50293164, 60 R.C.S. 131, 55 D.L.R. (2d) 461

D'Astous c. *Sesno,* [2001] R.J.D.T. 85, D.T.E. 2001T-25 (C.Q.)

Dion-Viens c. *Université Laval*, [2007] C.A.I. 173, conf. par 2008 QCCQ 640

Dumoulin c. *Gravel (Clinique de denturologie Rémi Gravel et Ass.)*, D.T.E. 2006T-26, AZ-50344142 (C.S.)

Employés du transport local et industries diverses, section locale 931 et United Parcel Service Canada, [2003] R.J.D.T. 1861, D.T.E. 2003T-1129 (T.A.), inf. par J.E. 2006-1121, D.T.E. 2006T-519 (C.S.)

Entreprises Cara Ltée et Association internationale des machinistes et des travailleurs de l'aéroastronautique, loge 987, [1984] T.A. 10, D.T.E. 84T-26

Fairmont Le Reine Élizabeth et Syndicat des travailleuses et travailleurs de l'Hôtel Le Reine Élizabeth (C.S.N.), D.T.E. 2004T-1168 (T.A.)

Fiset c. *Service d'administration P.C.R. Ltée*, (2003) R.J.D.T. 361 (C.T.)

Ford c. *Québec (Procureur général)*, [1988] 2 R.C.S. 712

Frenette c. *Métropolitaines (La), cie d'assurance-vie,* [1992] 1 R.C.S. 647

Furfaro et Costco Canada inc., D.T.E. 2000T-920 (C.T.)

Garaga inc. et Syndicat des salariés de garage (C.S.D.), [2002] R.J.D.T. 1802, D.T.E. 2002T-1100 (T.A.)

Gauthier c. *Nautilus Plus*, PV 98 14 62, 12 février 2002 (C.A.I.)

Genest et Québec (Directeur général des élections), D.T.E. 2007T-167 (C.F.P.)

Ghattas c. *École nationale de théâtre du Canada*, [2006] R.J.Q. 852, J.E. 2006-644 (C.S.)

Gilles et Ciba Spécialités chimiques Canada Inc., 2008 QCCRT 0134, D.T.E. 2008T-330

Godbout c. *Ville de Longueuil*, [1997] 3 R.C.S. 844

Hartco, l.p. c. Neulogic Sales Inc., B.E. 2006BE-177 (C.S.)

Investors Group c. Hudson, [1999] R.J.Q. 599 (C.S.)

Laboratoire de santé publique et Syndicat canadien de la fonction publique, section locale 2667, [1992] T.A. 23, D.T.E. 92T-34

Laforest c. *Caisse de dépôt et placement du Québec,* [2004] C.A.I. 31 (C.A.I.)

Laplante c. *Groupe de sécurité Garda inc.*, B.E. 2008BE-478 (C.Q.)

Lavoie c. *Pinkerton du Québec ltée*, [1996] C.A.I. 67

Legris c. *Repentigny (Ville de)*, [2007] C.A.I. 240 (C.A.I.)

Liberty Smelting Works (1962) Ltd. et Syndicat international des travailleurs unis de l'automobile, de l'aéronautique, de l'astronautique et des instruments aratoires d'Amérique (T.U.A.), local 1470, (1972) 3 S.A.G. 1039

Manufacture de Lambton ltée et Syndicat des salariés de Manufacture Lambton (CSD), D.T.E. 2003T-997 (T.A.)

Mascouche (Ville de) c. *Houle*, [1999] R.J.Q. 1894 (C.A.)

Métallurgistes unis d'Amérique, section locale 9414 et Nettoyeur Shefford inc., D.T.E. 2000T-272 (T.A.)

Minerais Lac Ltée-La mine Doyon et Métallurgistes unis d'Amérique, section locale 9291, D.T.E. 93T-928 (T.A.)

Montour Ltée et Syndicat des employés et employés de la Cie Montour (CSN), D.T.E. 2007T-195 (T.A.)

Multani c. *Commission scolaire Marguerite-Bourgeoys*, [2006] 1 R.C.S. 256

Paquet c. *Société des alcools du Québec*, [2007] C.A.I. 160 (C.A.I.), conf. par [2008] R.J.D.T. 1079 (C.Q.)

Personnelle-vie (La), corp. d'assurances c. *Cour du Québec*, [1997] R.J.Q. 2296, J.E. 97-1583 (C.S.)

Philips Électronique Ltée et Syndicat des travailleurs unis de l'électricité, radio et machinerie du Canada, section locale 565, [1991] T.A. 139, D.T.E. 91T-294

Poulies Maska inc. et Syndicat des employés de Poulies Maska inc., D.T.E. 2001T-620, AZ-01141163 (T.A.)

Praderes c. *Les Immeubles de la Montagne Ste-Catherine (1974) inc.*, PV 97 17 29, 4 avril 2001 (C.A.I.)

Pratt & Whitney Canada et Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleuses et travailleurs du Canada (TCA-Canada), D.T.E. 2005T-212 (T.A.)

Québec (Ministère du Revenu) et Syndicat de la fonction publique du Québec (Gouvernement du Québec (Ministère du Revenu) et Syndicat de la fonction publique du Québec), D.T.E. 99T-645 (T.A.)

R. c. *Gauthier*, [1999] R.J.Q. 2103, J.E. 99-1521 (C.Q.)

R. c. *Solomon*, [1996] R.J.Q. 1789 (C.A.)

R. c. *Tremblay*, J.E. 2001-1310, AZ-01031335 (C.Q.), conf. par B.E. 2003BE-315 (C.A.)

Regroupement des Comités Logement et Association de locataires du Québec c. Corporation des propriétaires immobiliers du Québec, rapport d'enquête, [1995]

C.A.I. 370, AZ-95151509 (C.A.I.)

Regroupement des travailleuses et travailleurs du Québec et Sécur (division guichets automatiques), [2002] R.J.D.T. 846 (T.A.)

Roy c. *Saulnier,* [1992] R.J.Q. 2419 (C.A.)

Royal & Sun Alliance du Canada c. *Québec (Ministère de la Sécurité publique)*, [2004] C.A.I. 345 (C.A.I.)

Section locale 143 du Syndicat canadien des communications, de l'énergie et du papier c. *Goodyear Canada inc.*, [2008] R.J.D.T. 24, J.E. 2008-97 (C.A.)

Service d'aide au consommateur et Reliable (La), compagnie d'assurance-vie, [1996] C.A.I. 406 (C.A.I.)

Service d'entretien Serca c. *Choquette*, D.T.E. 96T-699, J.E. 96-1239, AZ-96021446 (C.S.)

Société des alcools du Québec c. Syndicat des employés de magasins et de bureaux de la S.A.Q., [1983] T.A. 335

Société des alcools du Québec et Syndicat des travailleuses et travailleurs de la Société des alcools du Québec (SCFP), section locale 3535T, D.T.E. 2005T-229, AZ-50293590 (T.A.)

Srivastava c. *Hindu Mission of Canada (Québec) Inc.*, [2001] R.J.Q. 1111, J.E. 2001-1055 (C.A.)

St-Amant c. *Meubles Morigeau ltée,* [2006] R.J.Q. 1434 (C.S.)

Ste-Marie c. *Placements JPM Marquis inc.*, [2005] R.R.A. 295, J.E. 2005-711 (C.A.)

Syndicat canadien de la fonction publique, section locale 4140 et Centres jeunesse de l'Outaouais, D.T.E. 2005T-961, AZ-50338981 (T.A.)

Syndicat canadien des communications, de l'énergie et du papier et Induspac, division Corrugué inc., [2000] R.J.D.T. 837, D.T.E. 2000T-507 (T.A.)

Syndicat canadien des communications, de l'énergie et du papier, section locale 233 et Tembec inc., [2000] R.J.D.T. 1285, D.T.E. 2000T-855 (T.A.)

Syndicat canadien des communications, de l'énergie et du papier, section locale 522 et C.A.E. Électronique ltée, [2000] R.J.D.T. 327, D.T.E. 2000T-157 (T.A.)

Syndicat catholique des ouvriers du textile de Magog inc., section locale 10 et DIFCO Tissus de performance inc., [2000] R.J.D.T. 877 (T.A.)

Syndicat de la fonction publique du Québec – Fonctionnaires et Québec (Ministère de l'Emploi et de la Solidarité sociale), D.T.E. 2008T-642 (T.A.)

Syndicat de l'enseignement des Deux Rives (SEDR-CSQ) et Commission scolaire des Navigateurs, D.T.E. 2007T-516, AZ-50433953 (T.A.)

Syndicat de l'industrie du journal du Québec inc. (distribution) (CSN) et Presse ltée (La), D.T.E. 2000T-1167 (T.A.)

Syndicat démocratique des employés de commerce Saguenay-Lac-St-Jean et Potvin & Bouchard inc., [2006] R.J.D.T. 221, D.T.E. 2006T-75 (T.A.)

Syndicat des cols bleus regroupés de Montréal, section locale 301 et Montréal (Ville de) (arrondissement Côte-St-Luc—Hampstead—Montréal-Ouest), [2005] R.J.D.T. 1068, D.T.E. 2005T-507 (T.A.)

Syndicat des cols bleus regroupés de Montréal, section locale 301 (S.C.F.P.) et La Ronde (Six Flags), D.T.E. 2004T-1124 (T.A.)

Syndicat des employés de bureau de Thetford Mines et Thetford Mines (Ville de), D.T.E. 2005T-254 (T.A.)

Syndicat des employés de l'aluminerie de Baie-Comeau (CSN) et Alcoa ltée (Aluminerie de Baie-Comeau), D.T.E. 2005T-608, AZ-50319506 (T.A.)

Syndicat des employés des Aciers Atlas (C.S.N.) et Aciers Atlas, Une Division de Rio Algom Ltd., D.T.E. 83T-478, AZ-83141237 (T.A.)

Syndicat des employées et employés de la Société des casinos du Québec, section unité générale (CSN) et Société des casinos du Québec, D.T.E. 2006T-394, AZ-55000105 (T.A.)

Syndicat des employées et employés de métiers d'Hydro-Québec, section locale 1500 — SCFP (FTQ) et Hydro-Québec, D.T.E. 2009T-273 (T.A.)

Syndicat des employées et employés de techniques professionnelles et de bureau d'Hydro-Québec, section locale 2000 (SCFP/FTQ) et Hydro-Québec, D.T.E. 2005T-881 (T.A.)

Syndicat des employées et employés professionnels et de bureau, section locale 575 et Caisse Desjardins Thérèse-de-Blainville (D.D.), D.T.E. 2009T-170 (T.A.)

Syndicat des employées et employés professionnels et de bureau, section locale 57 et Caisse populaire St-Stanislas de Montréal, [1999] R.J.D.T. 350, D.T.E. 99T-59 (T.A.)

Syndicat des employés municipaux de Beloeil (SCFP) et Beloeil (Ville de), D.T.E. 2007T-874 (T.A.)

Syndicat des employés municipaux de la Ville de Saguenay (CSN) et Saguenay (Ville de), D.T.E. 2005T-511 (T.A.)

Syndicat des fonctionnaires municipaux de Québec et Ville de Québec, [1995] T.A. 997, D.T.E. 95T-1337

Syndicat des professionnelles du Centre jeunesse de Québec (CSN) c. *Desnoyers,* [2005] R.J.Q. 414, J.E. 2005-428 (C.A.), inf. par 2008 QCCA 1911

Syndicat des professionnelles et professionnels des affaires sociales du Québec (C.S.N.) et Institut de réadaptation en déficience physique de Québec, D.T.E. 2004T-924, AZ-50270443 (T.A.)

Syndicat de professionnelles et professionnels du gouvernement du Québec et Québec (Ministère du Revenu), D.T.E. 2003T-582 (T.A.)

Syndicat des salariées et salariés de General Dynamics, produits de défense et systèmes tactiques — Canada inc. et General Dynamics, D.T.E. 2008T-904 (T.A.)

Syndicat des salariées et salariés de La Survivance et La Survivance, [2006] R.J.D.T. 1657, D.T.E. 2006T-875 (T.A.)

Syndicat des spécialistes et professionnels d'Hydro-Québec, section locale 4250 (SCFP-FTQ) et Hydro-Québec, [2007] R.J.D.T. 1172, D.T.E. 2007T-541 (T.A.)

Syndicat des travailleurs de Praxair (C.S.N.) et Praxair inc., D.T.E. 2002T-413 (T.A.)

Syndicat des travailleurs de la mine Noranda Inc. Et Métallurgie du cuivre Noranda, fonderie Horne, D.T.E. 95T-1217 (T.A.)

Syndicat des travailleurs de l'énergie et de la chimie, section locale 107 c. *Laurin*, D.T.E. 91T-841, AZ-91029087 (C.S.)

Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.) c. *Trudeau*, [1999] R.J.Q. 2229, [1999] R.J.D.T. 1075 (C.A.)

Syndicat des travailleurs unis du Québec — STUQ (FTQ) et Pomatek inc., D.T.E. 2007T-784, AZ-50448279 (T.A.)

Syndicat des travailleuses et travailleurs de la Fabrique Notre-Dame — CSN et Fabrique de la paroisse Notre-Dame, D.T.E. 2006T-56 (T.A.)

Syndicat des travailleuses et travailleurs de Resto-Casino de Hull (F.E.E.S.P.-C.S.N.) (section Hilton Lac Leamy) et Hilton Lac Leamy, D.T.E. 2004T-811 (T.A.)

Syndicat du personnel de soutien de la Seigneurie des Mille-Îles (CSN) et Commission scolaire de la Seigneurie-des-Mille-Îles, D.T.E. 2008T-149 (T.A.)

Syndicat international des travailleurs de la boulangerie, confiserie et du tabac, section locale 476 F.A.T.-C.I.O.-C.T.C. et Walter M. Lowney Co., [1983] T.A. 665, D.T.E. 83T-423

Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleuses et travailleurs du Canada et BMW Canbec, D.T.E. 2007T-697, AZ-50441929 (T.A.)

Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleuses et travailleurs du Canada (TCA-Canada) et Cummins Est du Canada, [2007] R.J.D.T. 1227, D.T.E. 2007T-678 (T.A.)

Syndicat national des employés de garage du Québec inc. et Sovea Auto ltée, D.T.E. 2002T-707, AZ-02141190 (T.A.), conf. par (C.A., 2003-10-21), 200-09-004301-021, SOQUIJ AZ-03019685

Syndicat national des travailleurs des pâtes et papiers de Donnacona inc. (CSN) et Produits forestiers Alliance inc. (Bowater), [2008] R.J.D.T. 958, D.T.E. 2008T-469 (T.A.)

Unidindon inc. et Syndicat des travailleurs d'abattoir de volaille de St-Jean-Baptiste (C.S.N.), D.T.E. 2000T-368 (T.A.) (Requête en révision judiciaire rejetée, [2000] R.J.Q. 2064, J.E. 2000-1273(C.S.), conf. par D.T.E. 2001T-206 (C.A.))

Union des employées et employés de service, section locale 800 et Collège Marie de France, [2004] R.J.D.T. 1284, D.T.E. 2004T-645 (T.A.)

Union des routiers, brasserie, liqueurs douces et ouvriers de diverses industries, section locale 1999 et Brasserie Labatt ltée (Montréal), [1999] R.J.D.T. 648, D.T.E. 99T-402 (T.A.)

Université A et Syndicat des professeures et professeurs de l'Université A (SPPUA), D.T.E. 2007T-601 (T.A.)

Vifan Canada inc. et Syndicat des travailleuses et travailleurs de Vifan Canada inc. (CSN), D.T.E. 2007T-698, AZ-50445314 (T.A.)

Ville de Montréal c. *Association des pompiers de Montréal Inc.*, D.T.E. 90T-323 (T.A.)

X. et Komdresco Canada inc., D.T.E. 95T-1376 (C.A.I.)

X. c. *Laval (Société de transport de la Ville de)*, [2001] C.A.I. 226 (C.A.I.), conf. par *Laval (Société de transport de la Ville de)* c. *X.*, [2003] C.A.I. 667 (C.Q.)

X. et Services aux marchands détaillants ltée, [1996] C.A.I. 408, conf. par J.E. 2003-597, A.I.E. 2003AC-25, [2003] C.A.I. 667 (C.Q.)

Jurisprudence canadienne

1267623 Ontario Inc. v. *Nexx Online Inc.*, 46 B.L.R. (2d) 317, 45 O.R. (3d) 40, [1999] O.J. No. 2246 (Ontario Superior Court of Justice)

B. (R.). c. *Children's Aid Society of Metropolitan Toronto*, [1995] 1 R.C.S. 315

Briar c. *Conseil du Trésor (Solliciteur général du Canada - Service correctionnel)*, 2003 CRTFP 3

Brunswick News Inc. v. *Langdon,* 2007 NBQB 424, 858 A.P.R. 325, 334 N.B.R. (2d) 325

Camosun College v. *Canadian Union of Public Employees Local 2081*, [1999] B.C.C.A.A.A. 490

Canada (Commissaire à l'information) c. *Canada (Commissaire de la Gendarmerie royale du Canada)*, [2003] 1 R.C.S. 66

C.S. Gannon c. Conseil du Trésor (Défense nationale), 2002 CRTFP 32

Dagg c. *Canada (Ministre des Finances)*, [1997] 2 R.C.S. 403

Davison v. *Nova Scotia Construction Safety Assn.*, 2005 CarswellNS 683, 55 C.H.R.R. D/327 (Nova Scotia Board of Inquiry)

Dickason c. *Université de l'Alberta,* [1992] 2 R.C.S. 1103

Di Vito v. *MacDonald Dettwiler & Associates Ltd*, [1996] B.C.W.L.D. 2036

Douglas/Kwantlen Faculty Assn. c. *Douglas College*, [1990] 3 R.C.S. 570

Eastmond c. *Canadian Pacific Railway*, 2004 CF 852

Hunther c. *Southam Inc.*, [1984] 2 R.C.S. 145

Inform Cycle Ltd. v. *Rebound Inc.*, (2006), [2007] 3 W.W.R. 556, 2006 ABQB 825, 2006 CarswellAlta 1578, 68 Alta. L.R. (4th) 185 (Alta. Master)

International Association of Bridge, Local Union no. 97, and Structural and Ornamental Ironworkers and Office and Technical Employees' Union, Local 15, (1997) B.C.C.A.A.A. No. 630

Janzen c. Platy Enterprises Ltd., [1989] 1 R.C.S. 1252

Klein v. *Law Society of Upper Canada*, (1985) 50 O.R. (2d) 118 (Ontario Superior Court of Justice, Divisional Court)

Krain v. *Toronto Dominion Bank,* [2002] C.L.A.D. No. 406 (Can. Arb. Bd.)

Lac Minerals Ltd. c. *International Corona Resources Ltd.*, (1989) 2 R.C.S. 574

Lavigne c. *Syndicat des employés de la fonction publique de l'Ontario*, [1991] 2 R.C.S. 211

Milsom v. *Corporate Computers Inc.* (2003), 17 Alta. L.R. (4th) 124 (Alta Q.B.)

Pharand Ski Corp. v. Alberta, (1991) 37 C.P.R. (3d) 288 (ABQB)

R. v. *Bahr*, [2006] A.J. No. 1776, 434 A.R. 1 (Alberta Provincial Court)

R. c. *Beare*, [1988] 2 R.C.S. 387

R. c. *Colarusso*, [1994] 1 R.C.S. 20

R. c. *Duarte*, [1990] 1 R.C.S. 30

R. c. *Dyment*, [1988] 2 R.C.S. 417

R. c. *Edwards*, [1996] 1 R.C.S. 128

R. c. *Edwards Books and Art Ltd.*, [1986] 2 R.C.S. 713

R. v. *Giles*, [2007] B.C.J. No. 2918 (British Columbia Supreme Court)

R. c. *M. (M.R.)*, [1998] 3 R.C.S. 393

R. c. *Morgantaler*, [1988] 1 R.C.S. 30

R. c. *Morin*, [1992] 1 R.C.S. 771

R. c. *Oakes,* [1986] 1 R.C.S. 103

R. c. *Osolin*, [1993] 4 R.C.S. 595

R. v. *Weir*, [1998] 8 W.W.R. 228, 59 Alta. L.R. (3d) 319 (ABQB)

R. c. *Wong*, [1990] 3 R.C.S. 36

*Re Amalgamated Electric Corp. Ltd. (Markham) and International Brotherhood of Electrical Workers, Local 159*0 (1974), 6 L.A.C. (2d) 28 (Ont. Arbitration Board)

Re Inco Metals Co. and United Steelworkers (1978), 18 L.A.C. (2d) 420 (Ont. Arbitration Board)

Re Johnson Matthey & Mallory Ltd. and Precious Metal Workers Union, Federal Local 24739 (1975), 10 L.A.C. (2d) 354 (Ont. Arbitration Board)

Re Lornex Mining Corp. and United Steelworkers, Local 7619 (1983), 14 L.A.C. (3d) 169 (B.C. Arbitration Board)

Re United Automobile Workers, local 444 and Chrysler Corporation of Canada Limited (1961), 11 L.A.C. 152 (Ont. Arbitration Board)

Re United Electrical Workers, local 504 and Canadian Westinghouse Co. Ltd. (1964), 15 L.A.C. 348 (Ont. Arbitration Board)

Re University Hospital and *London & District Service Worker's Union*, Local 220 (1981), 28 L.A.C. (2d) 294 (Ont. Arbitration Board)

Robichaud c. *Canada (Conseil du trésor),* [1987] 2 R.C.S. 84

Rodriguez c. *Colombie-Britannique (Procureur général)*, [1993] 3 R.C.S. 519

St. Mary's Hospital and *H.E.U. (Re)* (1997), 64 L.A.C. (4th) 382 (Ont. Arbitration Board)

Telus Mobility and T.W.U. (Re) (2001), 102 L.A.C. (4th) 239 (Can. Arbitration Board)

Jurisprudence américaine

Borland Int'l, Inc. v. *Eubanks*, Cal. Sup. Ct., Civ. Case No. 123059 (Santa Cruz 1992)

Commonwealth of Pennsylvania v. *Proetto*, 2001 Pa. Super 95, 771 A.2d 823, 92 A.L.R.5th 681 (2001), inf. en partie par 567 Pa. 667, 790 A.2d 988 (2002)

Garrity v. *John Hancock Mut. Life Ins. Co.*, Civ. Act. No. 00-12143-RWZ, 2002 U.S.Dist. Lexis 8343 (D. Mass., May 7, 2002)

Guest v. *Leis*, 255 F.3d 325 (6th Cir. 2001)

Leventhal v. *Knapek*, 266 F.3d 64 (2d Cir. 2001)

McLaren v. *Microsoft Corp.*, 1999 WL 339015 (Tex.App.-Dallas)

Marobie-FL, Inc. v. *National Ass'n of Fire Equipment Disributors. (NAFED)*, 983 F. Supp. 1167 (N.D. Ill. 1997)

People v. *Eubanks*, 927 P.2d 310 (Cal. 1996)

Smyth v. *Pillsbury Co.*, 914 F. Supp. 97 (U.S. Dist. Ct. E.D. Penn. 1996)

Thygueson v. US Bancorp, No. CV-03-467-ST, 2004, WL 2066746 (D.OR. Sept. 15, 2004)

United States v. *Angevine*, 281 F.3d 1130 (10th Cir. 2000)

United States v. *Charbonneau*, 979 F. Supp. 1177 (S.D. Ohio 1997)

United States v. *Lifshitz*, 369 F.3d 173 (2d Cir. 2004)

United States v. *Long*, 64 M.J. 57 (C.A.A.F., 2006)

United States v. *Maxwell*, 42 M.J. 568 (A.F.C.C.A. 1995), inf. en partie par 45 M.J. 406, 1997 WL 643294 (A.F.C.C.A. 1997)

United States v. *Munroe*, 52 M.J. 326 (C.A.A.F. 2000)

United States v. *Slanina*, 283 F.3d, 670 (5th Cir. 2002)

United States v. *Warshak*, 490 F.3d 455 (6th Cir. 2007), inf. par No. 06-4092, 2008

WL 2698177, 2008 U.S. App. LEXIS 14717 (6th Cir. July 11, 2008)

United States v. *Ziegler*, 497 F.3d. 890 (9th Cir. 2007)

Jurisprudence française

C.A. Douai (ch. soc.), 30 mars 2007, n° R.G. 06/02138

Soc. 2 octobre 2001, *Bull. civ.* V, no. 291

Soc., 17 mai 2005, *Bull. civ.* V, n° 165

Soc. 18 octobre 2006, pourvoi n° 04-47400

Soc. 18 octobre 2006, pourvoi n° 04-48025

Soc., 30 mai 2007, pourvoi n° 05-43102

Colmar, 29 mai 2008, n° 07/03314 (Cour d'appel)

Douai, 26 nov. 2004, *M. Philippe X. c/ S.A. Laboratoires Pharmaceutiques Rodael, M. Paul E.,* n° RG : 04/00709

Trib. Gr. Inst. Marseille, 1e ch. Civ., 11 juin 2003, *SA Escota c/ Société Lycos, Société Lucent Technologies et M. N. B.*, conf. par CA Aix-en-Provence, 2^{e} ch., 13 mars 2006, pourvoi no. 2006/170

Trib. Gr. Inst. Paris, 19 octobre 2006, *Mme H.P. c/ SARL Google France et Google Inc.,* n° RG 06/58312

Jurisprudence étrangère

Ansell Rubber Co. Pry v. *Allied Bubber Industries Pty Ltd. (1967),* [1967] V.Q. 37, [1972] R.P.C. 811 (Australia Vic. Sup. Ct.)

Coco v. *A.N. Clark (Engineers) Ltd.*, [1969] R.P.C. 41 (Chancery Division, England and Wales)

Table de la doctrine

Monographies et ouvrages collectifs

BACARD, A., *The Computer Privacy Handbook*, Berkeley (Calif.), Peachpit Press, 1995, 274 p.

BEAUDOIN J.-L. et P. DESLAURIERS, *La responsabilité civile*, 7e ed., Cowansville, Éditions Yvon Blais, 2007, 2016 p.

BERNIER, L., L. GRANOSIK et J.-F. PEDNEAULT, *Les droits de la personne et les relations du travail*, Cowansville, Éditions Yvon Blais, 1997, feuilles mobiles, à jour au 10 décembre 2008 (no.23, Nov. 2008).

BOURGAULT, J., *Le harcèlement psychologique au travail: les nouvelles dispositions de la Loi sur les normes et leur intégration dans le régime légal préexistant*, Montréal, Wilson & Lafleur, 2006, 190 p.

BROWN, D. J. M. et D. M. BEATTY, *Canadian Labour Arbitration*, 4th edition, Aurora (Ont.), Canada Law Books, 2006, feuilles mobiles, à jour au 23 mars 2009 (no.10, MAR:2009).

BRUN, H. et G. TREMBLAY, *Droit constitutionnel*, 5e éd., Cowansville, Éditions Yvon Blais 2008, 1548 p.

CÔTÉ, S., *NETendances 2007, Évolution de l'utilisation d'Internet au Québec depuis 1999*, version abrégée, Montréal, CEFRIO, 2007.

CÔTÉ, S., *NETendances 2007, Évolution de l'utilisation d'Internet au Québec depuis 1999*, version intégrale, Montréal, CEFRIO, 2007.

D'AOUST, C., L. LECLERC et G. TRUDEAU, *Les mesures disciplinaires : étude jurisprudentielle et doctrinale,* Montréal, École des relations industrielles, Université de Montréal, 1982, 484 p.

DELEURY, É. et D. GOUBAU, *Le droit des personnes physiques*, Cowansville, Les Éditions Yvon Blais, 1994, 651 p.

FLYNN, F., *Instant Messaging Rules*, New York, AMACOM, 2004, 210 p.

KLEIN, K. et V. GATES, *Privacy in Employment: Control of Personal Information in the Workplace*, Toronto, Thompson Carswell, 2005, 136 p.

GAGNON, R. P., *Le Droit Du Travail Du Québec*, 8e éd., Cowansville, Éditions Yvon Blais, 2008, 972 p.

LAJOIE, A., *Pouvoir disciplinaire et tests de dépistages de drogues en milieu de travail: illégalité ou pluralisme*, Cowansville, Éditions Yvon Blais, 1995, 91 p.

LAMOTHE, M., *La renonciation à l'exercice des droits et libertés garantis par les chartes*, Cowansville, Les Éditions Yvon Blais, 2007, 247 p.

LIMPERT, P. B., *Technology Contracting: Law, Precedents and Commentary*, Toronto, Carswell, 2009, feuilles mobiles, à jour en 2009 (release 2009-1).

LYON-CAEN, G., *Les libertés publiques et l'emploi*, Rapport pour le ministre du Travail, de l'Emploi et de la Formation professionnelle, Rapport officiel, Paris, La documentation française, 1992.

MCNAIRN, C. H.H. and A. K. SCOTT, *A Guide to the Personal Information Protection and Electronic Documents Act*, Markham (Ont.), Lexis Nexis, 2007, 268 p.

MCNAIRN, C. H.H. and A. K. SCOTT, *Privacy Law in Canada*, Markham (Ont.), Butterworths, 2001, 334 p.

MORIN, F. et J.-Y. BRIÈRE, *Le droit de l'emploi au Québec*, 3e éd., Montréal, Wilson et Lafleur, 2006, 1780 p.

TRUDEL, P., F. ABRAN, K. BENYEKHLEF et S. HEIN, *Droit du cyberespace*, Montréal, Thémis, 1997, 1296 p.

TURNBULL, I. J., *Privacy in the Workplace: The Employment perspective*, Toronto, CCH, 2004, 374 p.

Articles de revue et études d'ouvrages collectifs

BICH, M.-F., « Le contrat de travail : Code civil du Québec, Livre cinquième, titre deuxième, chapitre septième (articles 2085-2097 C.c.Q.) », dans Barreau du Québec et Chambre des notaires du Québec (dir.), *La réforme du Code civil : obligations, contrats nommés*, t. 2, Sainte-Foy, P.U.L., 1993, p. 741-796

CAIN, M. W., D. M. SMITH, and B. BURTON, « Management update: wake up to the realities of instant messaging », October 19, 2005, Gartner Inc. (Research : G00133673), en ligne:

http://www3.villanova.edu/gartner/research/133600/133673/133673.pdf

CASSER, K. L., « Employers, Employees, E-mail and The Internet », *The Internet and Business : A Lawyer's Guide to the Emerging Legal Issues*, Washington D.C., The Computer Law Association Inc., 1996

DELWAIDE, K., « La protection de la vie privée et les nouvelles technologies: l'accès au courrier électronique des employés par un employeur », dans S.F.P.B.Q., *Congrès annuel du Barreau du Québec (1997),* Cowansville, Éditions Yvon Blais, p. 627-666

D'AOUST, C., « L'électronique et la psychologie dans l'emploi », dans D. NADEAU & B. PELLETIER (dir.), *Relation d'emploi et droits de la personne : évolution et tensions!*, Cowansville, Éditions Yvon Blais, 1994, p. 35-49

DUHAIME, L., « La protection des renseignements personnels en milieu de travail », dans S.F.P.B.Q., vol. 258, *Vie privée et protection des renseignements personnels (2006)*, Cowansville, Éditions Yvon Blais, p. 83-104

ELTIS, K., « La surveillance du courrier électronique en milieu de travail : le Québec succombera t-il à l'influence de l'approche américaine », (2006) 51 *R.D. McGill* 475-502, en ligne : http://lawjournal.mcgill.ca/documents/1224865238_Eltis.pdf

ELTIS, K., « The Emerging American Approach to E-Mail Privacy in the Workplace: Its Influence on Developing Case Law in Canada and Israël: Should Others Follow Suit? » (2002-2003) 24 *Comp. La. L. & Pl'y J.* 487-524

GAUTRAIS, V., « Afin d'y voir clair, Guide relatif à la gestion des documents technologiques », Fondation du Barreau du Québec, Montréal, novembre 2005, en ligne : http://www.fondationdubarreau.qc.ca/pdf/publication/Guidetech_FR.pdf

GEIST, M., « Computer and E-mail Workplace Surveillance in Canada: The Shift from reasonable expectation of privacy to reasonable surveillance », rapport préparé pour le Conseil Canadien de la Magistrature, Mars 2002, en ligne: http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_Surveillance_2002_en.pdf, traduction française disponible en ligne: http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_Surveillance_2002_fr.pdf

HEBERT, W. A., «The Electronic Workplace: To Live Outside the Law You Must Be Honest», (2008) 12 *Employee Rts. & Emp. Pol'y J.* 49-104

Éric LACROIX, *NETendances 2002, Utilisation d'Internet au Québec,* version abrégée, Montréal, CEFRIO, Janvier 2003

LANGELIER, R., « La protection de la vie privée par la Commission d'accès à l'information : quelle vie privée? Quelle protection? En fonction de quels intérêts? », dans S.F.P.B.Q., vol. 233, *Développements récents en droit de l'accès à l'information (2005)*, Éditions Yvon Blais, Cowansville, 2005, 149-220

LAPLANTE, L., « L'Internet et l'emploi » dans F.P.B.Q., *Congrès annuel du Barreau du Québec (1997),* Cowansville, Éditions Yvon Blais, p. 709-727

LASPROGATA, G., « Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada », 2004 *Stan. Tech. L. Rev.* 4, en ligne: http://stlr.stanford.edu/pdf/Lasprogata-RegulationElectronic.pdf

LEFEBVRE, S., « Naviguer sur Internet au travail : et si on nageait en eaux trouble? », dans S.F.P.B.Q., vol. 293, *Développements récents en droit du travail (2008)*, Cowansville, Éditions Yvon Blais, p. 51-128

LE MEUR, L., « Les webblogs et leur utilisation en interne pour les entreprises », dans *Six Apart SA*, France, 2006, en ligne : http://loiclemeur.com/english/images/KM_loic2.pdf

MÉLIN, M. et D. MELINSON, « Salarié, employeur et données informatiques: brefs regards croisés sur une pièce à succès », *Revue Lamy Droit de l'immatériel*, Janvier 2007, Vol. 23, p. 69-74

MORGAN, C., « Employer Monitoring of Employee Electronic Mail and Internet Use », (1999) 44 *R. D. McGill* 849-902

MORGAN, C., « Monitoring Employee — Electronic Mail and Internet Use: Balancing Competing Rights», dans Vincent GAUTRAIS (dir.), *Droit du commerce électronique*, Montreal, Éditions Thémis, 2002, p. 171-211

PERREAULT, R., « L'adoption d'une politique d'utilisation du courriel et d'Internet: où est le bogue? », dans S.F.P.B.Q., vol. 134, *Développements récents en droit du travail (2000),* Cowansville, Éditions Yvon Blais, p. 71-97

POIRIER, M.-A., « Employer Monitoring of the Corporate E-Mail System : How Much Privacy Can Employees Reasonably Expect? », (2002) 60 *U. Toronto Fac. L. Rev.* 85-104

SAINT-ANDRÉ, Y., « Le respect du droit à la vie privé au travail : mythe ou réalité? », dans S.F.P.B.Q., vol. 205, *Développements récents en droit du travail (2004),* Cowansville, Éditions Yvon Blais, p. 51-80

TRUDEL, P., « *La responsabilité sur Internet* », Centre de recherche en droit public, Université de Montréal, 2002

TURMEL, B., « Le droit de fouille en milieu de travail » dans Denis NADEAU et B. PELLETIER (dir.), *Relation d'emploi et droits de la personne; évolution et tensions!,* Actes du colloque de la faculté de droit de l'Université d'Ottawa tenu le 12 mars 1993, Cowansville, Éditions Yvon Blais, 1994, p. 51-71

VEILLEUX, D., « Le droit à la vie privée – sa portée face à la surveillance de l'employeur », (2000) 60 *R. du B.* 1-46

WARREN S. D. and L. D. BRANDEIS, « The right to privacy », (1890) *4 Harvard L.Rev.* 193, en ligne: http://www.abolish-alimony.org/content/privacy/Right-to-Privacy-Brandeis-Warren-1890.pdf

WEN H. J. and al., « Internet Usage Monitoring in the Workplace : Its Legal Challenges and Implementation Strategies », *Information Systems Management,* (2007) 24 (n° 2), p.185-196, en ligne: http://road.uww.edu/road/peltierj/Privacy/Internet%20usage%20monitoring%20in%20the%20workplace.pdf

Documents des organismes privés ou paragouvernementaux

AMERICAN MANAGEMENT ASSOCIATION (AMA) AND THE EPOLICY INSTITUTE, *2006 Workplace E-Mail, Instant Messaging & Blog Survey*, États-Unis, 2006, résumé en ligne: http://www.epolicyinstitute.com/survey2006Summary.pdf

AMERICAN MANAGEMENT ASSOCIATION (AMA) AND THE EPOLICY INSTITUTE, *2007 Electronic Monitoring & Surveillance Survey*, États-Unis, 2007, résumé en ligne: http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf

CEFRIO, *Les enjeux du télétravail au Québec – Rapport de recherche*, Québec, Mai 2001.

CEFRIO, *NetQuébec 2008 – Portrait de l'utilisation des TI et d'Internet au Québec*, Québec, 2008, en ligne : http://cefrio.qc.ca/fckupload/DEPL_netquebec_web_SECUR.pdf

CROP, « Visite d'Internet au Travail », dans *CROP-Express*, #35, Québec, Février 2007, en ligne : http://www.orhri.org/presse/2007/070402_CROP_internet-trav.pdf

HARRIS INTERACTIVE, *Websense, Inc. Web@Work Survey 2006*, New York, mai 2006, en ligne : http://www.websense.com/global/en/PressRoom/MediaCenter/Research/webatwork/Employee_Computing.pdf

IBM, *IBM Internet Security Systems – X-Force 2007 Trend & Risk Report*, États-Unis, IBM Global Technology Services, January 2009, en ligne : http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf

IPSOS REID, *The 2006 Canadian Inter@ctive Reid Report*, Canada, 2006, 6 p.

ISEE, « Des TIC de plus en plus diversifiées dans les entreprises », dans *INSEE Première*, no. 1126, France, Mars 2007

PARME COMMUNICATION ET INTERNET SECURITY SYSTEMS, *Le nombre de sites web aux contenus illégaux ou extrémistes a augmenté de 42% en 2005*, Communiqué de presse, France, 5 décembre 2005, en ligne : http://www.parmecommunication.com/outils/presse/read.php?page=116&client=18&message=467

RADICATI GROUP, INC. AND MIRAPOINT, INC., *Corporate Email User Habits*, California, September 2005, en ligne: http://www.imerja.com/files/file/Reports/Radicati%20Group/Email%20user%20habits.pdf

SERVICE DES ÉTUDES ET DES STATISTIQUES INDUSTRIELLES (SESSI), DiGITIP, « L'utilisation des TIC dans les entreprises », dans *Le 4 Pages des statistiques industrielles*, No. 201, France, janvier 2005

Documents des organismes publics

BUREAU OF LABOUR STATISTICS, *Computer and Internet Use at Work in 2003*, United States Department of Labor, Octobre 2003, en ligne: http://www.bls.gov/news.release/pdf/ciuaw.pdf

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Conclusions en vertu de la *Loi sur la protection des renseignements personnels, Surveillance indue des comptes de courrier électronique d'employés* (2001-2002), en ligne : http://www.priv.gc.ca/cf-dc/pa/2001-02/pa_200102_05_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Conclusions en vertu de la *Loi sur la protection des renseignements personnels, Le gouvernement a le droit de surveiller l'utilisation de ses systèmes de courrier électronique* (2005-2006), en ligne : http://www.privcom.gc.ca/cf-dc/pa/2005-

06/pa_200506_06_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Conclusions en vertu de la *Loi sur la protection des renseignements personnels, Surveillance des courriels d'un employé se révèle appropriée* (2007-2008), en ligne http://www.priv.gc.ca/cf-dc/pa/2007-08/pa_200708_05_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2003-114 – *Un employé s'oppose à l'utilisation de caméras vidéo numériques de surveillance par la compagnie*, en ligne : http://www.priv.gc.ca/cf-dc/2003/cf-dc_030123_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2003-160 – *Une entreprise de télécommunications surveillance les appels des clients*, en ligne : http://www.priv.gc.ca/cf-dc/2003/cf-dc_030416_5_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2004-264 – *Caméras vidéo et cartes magnétiques au travail,* en ligne : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040219_01_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2004-265 – *Caméras vidéo au travail,* en ligne : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040219_02_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2004-268 – *La surveillance électronique ne donne aucun résultat, mais la pratique est fortement découragée*, en ligne : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040412_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2004-269 – *L'employeur embauche un enquêteur privé pour exercer une surveillance vidéo d'un employé*, en ligne : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040423_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2004-273 – *À la suite de l'installation de caméras de surveillance sur les lieux de travail, une compagnie de radiodiffusion s'engage à informer ses employés des fins de la collecte et à adopter une politique concernant leur utilisation*, en ligne : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040518_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA,

Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2004-279 – *La surveillance des employés au travail*, en ligne : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040726_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2005-290 – *La surveillance des employés au travail,* en ligne : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040726_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2005-297 – *Courriels non sollicités pour fins de marketing*, en ligne : http://www.privcom.gc.ca/cf-dc/2005/297_050331_01_f.asp

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2006-351 – *Examen de l'utilisation des renseignements personnels recueillis au moyen d'un système mondial de localisation*, en ligne : http://www.priv.gc.ca/cf-dc/2006/351_20061109_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2007-372 – *Les communications aux courtiers en données exposent les faiblesses des mesures de sécurité en télécommunications* – http://www.privcom.gc.ca/cf-dc/2007/372_20070709_f.asp

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2007-379 – *L'état des toilettes amène la direction d'une entreprise à y exercer une surveillance*, en ligne : http://www.priv.gc.ca/cf-dc/2007/379_20070404_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, Résumé de conclusions d'enquête en vertu de la LPRPDÉ, n° 2007-387 – *Une station de télévision enregistre indûment la conversation téléphonique d'un employé*, en ligne : http://www.priv.gc.ca/cf-dc/2007/387_20061204_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Conférence sur la vie privée au travail*, discours de George Radwanski, Vancouver, 23 mai 2003, en ligne : http://www.privcom.gc.ca/speech/2003/02_05_a_030529_f.asp

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Des plaintes de harcèlement et de vandalisme justifient une surveillance* (2006-2007), en ligne : http://www.priv.gc.ca/cf-dc/pa/2006-07/pa_200607_05_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Fiche d'information - La protection des renseignements personnels au travail*, 19 février 2004, en ligne : http://www.privcom.gc.ca/fs-fi/02_05_d_17_f.asp

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Fiche d'information-Lignes directrices sur l'enregistrement des appels téléphoniques des clients,* révisé en juin 2008, en ligne : http://www.priv.gc.ca/fs-fi/02_05_d_14_f.cfm

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Guide à l'intention des entreprises et des organisations – Protection des renseignements personnels : vos responsabilités*, mars 2004, en ligne : http://www.priv.gc.ca/information/guide_f.pdf

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La vie privée au travail à l'ère d'Internet*, discours de George Radwanski, Toronto, 4 octobre 2002, disponible à http://www.privcom.gc.ca/speech/02_05_a_021004_2_f.asp

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Le respect de la vie privée à l'ère d'Internet*, extrait de l'allocution de George Radwanski, Centre des relations industrielles de l'Université de Toronto et Lancaster House Publishing, 5e Conférence annuelle sur l'arbitrage en relations de travail, Toronto, 2 novembre 2001, en ligne : http://www.privcom.gc.ca/speech/02_05_a_011102_f.asp

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Nouvelle loi, nouvelle époque*, Allocution de George Radwanski à la Conférence de l'Université de Toronto et Lancaster House sur les derniers développements en matière de vie privée au travail, Toronto, 6 avril 2001, en ligne : http://www.privcom.gc.ca/speech/02_05_a_010406_f.asp

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Trouver le bon équilibre en ce qui concerne la protection de la vie privée au travail*, Allocution prononcée par Jennifer Stoddart, Toronto, 30 novembre 2006, en ligne : http://www.privcom.gc.ca/speech/2006/sp-d_061130_f.asp

COMMISSION DES DROITS DE LA PERSONNE ET DE LA JEUNESSE, *Filature et surveillance des salariés absents pour raison de santé : conformité à la charte*, Cat. 2.115.21, Québec, Avril 1999, en ligne : http://www.cdpdj.qc.ca/fr/publications/docs/filature.pdf

COMMISSION DES DROITS DE LA PERSONNE ET DE LA JEUNESSE, *Fouilles des véhicules et effets personnels de travailleurs à la sortie d'une mine –*

compatibilité avec la Charte des droits et libertés de la personne, Cat. 2.115.11, Québec, Juin 1998, en ligne : http://www.cdpdj.qc.ca/fr/publications/docs/fouilles_vehicules.pdf

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), *La cybersurveillance sur les lieux de travail*, mars 2004, en ligne : http://www.cnil.fr/fileadmin/documents/approfondir/dossier/travail/cyber_conclusions.pdf

STATISTIQUE CANADA, « Commerce électronique et technologie », *Le Quotidien*, 24 avril 2008, en ligne : http://www.statcan.gc.ca/daily-quotidien/080424/dq080424a-fra.htm

STATISTIQUE CANADA, *Enquête canadienne sur l'utilisation d'Internet, utilisation d'Internet, selon le point d'accès, le sexe et le groupe d'âge, aux 2 ans (pourcentage), 2005 à 2007*, CANSIM : tableau 358-0124.

Mémoires de maîtrise ou doctorat

ALCATRAZ, P., *La notion de copie privée*, Mémoire de D.E.A. de Propriété intellectuelle, Nantes, Faculté de Droit et de Sciences politiques, Université de Nantes, 2002-2003

BLANCHETTE, F., *L'expectative raisonnable de vie privée et les principaux contextes de communications dans Internet*, thèse de maîtrise, Montréal, Faculté des études supérieures, Université de Montréal, 2001, en ligne : http://www.juriscom.net/documents/priv20040203.pdf

LENFANT, J., *Le droit à la vie privée s'étend-il à l'utilisation du courriel par un employé dans le cadre de ses fonctions?*, Montréal, Faculté des études supérieures, Université de Montréal, 2000, en ligne : http://www.juriscom.net/uni/etd/04/priv01.pdf

Sources Internet

BEAUDOIN, C., « Les travailleurs québécois considèrent que l'accès à Internet augmente la productivité », dans *Fiche de renseignements des Services Kelly – Résultats du sondage Internet – Canada*, 26 mars 2007, en ligne : http://www.kellyservices.ca/res/content/ca/services/fr/docs/quebec_internet_release_final_french.pdf

CARRIÈRE, L., « Les secrets de commerce: notions générales », 1996, *robic.ca*, en ligne : http://www.robic.ca/publications/Pdf/202-LC.pdf

D'AMOURS, L., « Croissance du télétravail: bonne nouvelle? », *technaute.com*, 28 mars 2007, en ligne : http://technaute.cyberpresse.ca/nouvelles/200703/28/01-11640-croissance-du-teletravail-bonne-nouvelle.php

DELWAIDE, K., « L'Internet en milieu de travail et les politiques et directives relatives à l'utilisation des nouvelles technologies », Montréal, *fasken.com*, 2001, en ligne : http://www.fasken.com/files/Publication/2bdfed9a-a187-4755-abc3-04fd5e0c6bb1/Presentation/PublicationAttachment/6bed511b-6037-4345-a9f6-09760d937b45/L_INTERNET_EN_MILIEU_DE_TRAVAIL.pdf

DELWAIDE K. et AYLWIN, A., « Leçons tirées de dix ans d'expérience : La Loi sur la protection des renseignements personnels dans le secteur privé du Québec », Conférence juridique canadienne et l'exposition commerciale de l'Association du Barreau canadien, Vancouver, Colombie-Britannique, 16 août 2005, en ligne : http://www.priv.gc.ca/information/pub/dec_050816_f.pdf

LEVIN, A., M. FOSTER, M. J. NICHOLSON et T. HERNANDEZ, « Under the Radar? The Employer Perspective on Workplace Privacy », Ryerson University, Juin 2006, en ligne: https://www.theprivacynetwork.org/SSN/CurrentPrivacyIssues/WorkplaceandEmployment/Documents%20and%20Links/Ryerson%20Report%20-%20Under%20the%20Radar.pdf

LOCKTON V. and R. S. ROSENBERG, *A preliminary Exploration of Workplace Privacy Issues in Canada*, report submitted to the Office of the Privacy Commissioner of Canada, University of British Columbia, April 10th, 2006, en ligne: http://www.cs.ubc.ca/~lockton/workplace.pdf

MICROSOFT, Rubrique des Bloggeurs de Microsoft France, en ligne : http://www.microsoft.com/france/blogs/blogs.mspx

PÉPIN, R., « Le statut juridique du courriel au Canada et aux États-Unis », (2001) 6-2 *Lex electronica*, en ligne : http://www.lex-electronica.org/articles/v6-2/pepin.htm

OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE (OQLF), « Le grand dictionnaire terminologique », en ligne : http://www.granddictionnaire.com

O'NEILL, A., « E-Mail can bounce back to hurt you », *CNN.com*, November 7, 2005, en ligne: http://www.cnn.com/2005/LAW/11/03/email.legal/

Robert RICHARDSON, « The 2008 CSI/FBI Computer Crime and Security Survey », États-Unis, en ligne: http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

WIKIPEDIA, « RSS (Format) », 2009, en ligne : http://fr.wikipedia.org/wiki/RSS_(format)

ANNEXE 1 – LISTE DE VÉRIFICATION PRÉALABLE

1. L'employé dispose-t-il d'une expectative raisonnable de vie privée dans le cadre de l'utilisation d'Internet au travail?

Facteurs d'appréciation de l'expectative raisonnable de vie privée	
Connaissance de la surveillance	
-Politique de surveillance : ☐ oui ☐ non -Avis et rappels : ☐ oui (fréquence : _____ mode : _____) ☐ non -Séances d'information : ☐ oui ☐ non -Pratique établie : ☐ oui (nb. d'années : _____) ☐ non	
Consentement à la surveillance	
☐ Consentement explicite Détails : _____ _____	☐ Consentement implicite Détails : _____ _____
Nature vulnérables des communications Internet	
Existence d'un mot de passe d'accès pour chaque employé : ☐ oui ☐ non	
Environnement de travail	
-L'employeur est-il propriétaire des outils informatiques? ☐ oui ☐ non -Nature du travail exercé par l'employé : _____ -L'employé a-t-il accès, dans le cadre de son travail, à des renseignements secrets ou de nature délicate? ☐ oui (lesquels : _____) ☐ non -L'employé fait-il du télétravail? ☐ oui (fréquence : _____) ☐ non	

-Les dossiers ou fichiers surveillés contiennent-ils une mention « personnel » ou ont-ils été classés dans un dossier intitulé « personnel »? ☐ oui ☐ non

-Combien d'heures par semaine l'employé passe-t-il au travail ? _____ heures

-L'employeur collecte-t-il des « renseignements personnels » dans le cadre de la surveillance? ☐ oui (lesquels : _____) ☐ non

1. Quels sont les motifs sous-jacents à la surveillance de l'utilisation d'Internet au travail (critère de rationalité)?

Risques techniques	
Motif(s)	**Incident(s) ou doute(s) sérieux***
☐ Éviter l'encombrement du réseau Internet	
☐ Maintenir la sécurité du réseau, éviter les attaques extérieures (i.e. virus)	

* Si l'employeur a subit des incidents dans le passé ou entretient des doutes sérieux sur un ou plusieurs employés, fournir le détail.

Risques Juridiques	
Motif(s)	**Incident(s) ou doute(s) sérieux***
☐ Éviter le téléchargement ou la transmission de contenu préjudiciable ou illégal	
☐ Éviter la violation de propriété intellectuelle	
☐ Supprimer le harcèlement psychologique	

☐ Éviter la dissémination ou le vol d'information privilégiée et confidentielle	
☐ Protéger la vie privée, l'image et la réputation de l'entreprise	
☐ Éviter une baisse de productivité ou le vol de temps de la part des employés	

* Si l'employeur a subit des incidents dans le passé ou entretient des doutes sérieux sur un ou plusieurs employés, fournir le détail.

2. Comment l'employeur entend-t-il exercer la surveillance de l'utilisation d'Internet (critère de proportionnalité) ?

Nécessité de la surveillance de l'utilisation d'Internet
Autres mesures employées
Indiquer les mesures moins intrusives prises par l'employeur préalablement à la mise en place de la surveillance pour atteindre ses objectifs. _____ _____ _____ _____
Expliquer pourquoi ces mesures n'ont pas rapporté les résultats escomptés. _____ _____ _____ _____
Si l'employeur n'a pris aucune autre mesure préalable, expliquer pourquoi. _____ _____ _____ _____

Étendue de la surveillance	
Employés surveillés	
☐ Un ou quelques employés Nombre : _____ Raison de la sélection : _____ _____	☐ Tous les employés Raison de l'uniformité : _____ _____
Activités surveillées	
☐ Activités professionnelles ☐ Activités personnelles ☐ Courriel ☐ Navigation Web ☐ Utilisation des blogs ☐ Messagerie instantanée ☐ Contenu du disque dur de l'employé	☐ Toutes les activités Internet
Caractère continue de la surveillance	
☐ Surveillance ponctuelle ou épisodique Circonstances : _____ Mode de sélection au hasard : _____ _____	☐ Surveillance continue et permanente

Transparence de la surveillance	
Information données aux employés	
☐ Employé(s) surveillé(s) informé(s)	☐ Employé(s) surveillé(s) non informé(s)

Outil(s) d'information : ☐ Politique de surveillance ☐ Pamphlets ☐ Avis électroniques ☐ Séances d'information ☐ Autres : _____	
Consentement obtenu du ou des employés	
☐ Consentement obtenu ☐ Consentement explicite Détails : _____ _____ ☐ Consentement implicite Détails : _____ _____	☐ Consentement non obtenu
Pratique établie	
☐ Pratique établie Nb. d'années : _____ années	☐ Pratique non établie
Politique de surveillance de l'utilisation d'Internet	
☐ Politique de surveillance en vigueur Année d'adoption : _____ ☐ Négociée ☐ Non Négociée ☐ Avec syndicat ☐ Avec employés ☐ Distribuée à tous les employés ☐ Mise en pratique de la politique de manière constante et uniforme	☐ Aucune politique de surveillance en vigueur

Confidentialité de la surveillance
Sécurité et restriction d'accès aux résultats
Nombre d'employés ayant accès aux résultats de la surveillance : _____ Titre des employés ayant accès aux résultats de la surveillance : _____ _____ _____ _____ _____ _____
Sécurité de l'endroit où sont conservés les résultats de la surveillance (détailler) : _____ _____
Autres mesures prises par l'employeur pour restreindre l'accès aux résultats de la surveillance (détailler) : _____ _____